

10/527820  
Rec'd T/PTO 14 MAR 2005  
PCT/JP2004/010432

15. 7. 2004

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

REC'D 02 SEP 2004
WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日      2 0 0 4 年   7 月   2 日  
Date of Application:

出 願 番 号      特 願 2 0 0 4 - 1 9 7 4 5 3  
Application Number:  
[ST. 10/C]:      [ J P 2 0 0 4 - 1 9 7 4 5 3 ]

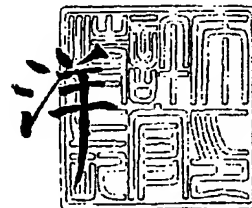
出   願   人      松 下 電 器 産 業 株 式 有 限 公 司  
Applicant(s):

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2 0 0 4 年   8 月 2 0 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川



出証番号   出証特 2 0 0 4 - 3 0 7 5 0 4 1

【書類名】 特許願  
【整理番号】 7048160027  
【提出日】 平成16年 7月 2日  
【あて先】 特許庁長官殿  
【国際特許分類】 G06F 15/00  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内  
    【氏名】 高木 佳彦  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内  
    【氏名】 菊地 隆文  
【特許出願人】  
    【識別番号】 000005821  
    【氏名又は名称】 松下電器産業株式会社  
【代理人】  
    【識別番号】 100105050  
    【弁理士】  
    【氏名又は名称】 鷲田 公一  
【先の出願に基づく優先権主張】  
    【出願番号】 特願2003-275672  
    【出願日】 平成15年 7月16日  
【手数料の表示】  
    【予納台帳番号】 041243  
    【納付金額】 16,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 9700376

**【書類名】 特許請求の範囲****【請求項1】**

機器からメモリデバイスに対するアクセス方法であって、  
前記機器が、  
前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、  
前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、  
前記メモリデバイスが、  
前記指定情報を受信するステップと、  
前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、  
前記検証にて成功した場合、前記処理命令を実行するステップと、  
を有するアクセス方法。

**【請求項2】**

機器からメモリデバイスに対するアクセス方法であって、  
前記機器が、  
前記メモリデバイスとで、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、  
前記可能領域情報を参照し、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、  
前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、  
前記メモリデバイスが、  
前記指定情報を受信するステップと、  
前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、  
前記検証にて成功した場合、前記処理命令を実行するステップと、  
を有するアクセス方法。

**【請求項3】**

機器からメモリデバイスに対するアクセス方法であって、  
前記機器が、  
前記メモリデバイスとで、検証用鍵を共有化するステップと、  
前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、  
前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、  
前記メモリデバイスが、  
前記指定情報を受信するステップと、  
前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、  
前記検証にて成功した場合、前記処理命令を実行するステップと、  
を有するアクセス方法。

**【請求項4】**

機器からメモリデバイスに対するアクセス方法であって、  
前記機器が、  
前記メモリデバイスとで、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、  
前記メモリデバイスとで、前記アクセス可能領域に対応した検証用鍵を共有化するステップと、  
前記可能領域情報を参照し、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、

前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、  
前記メモリデバイスが、  
前記指定情報を受信するステップと、  
前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、  
前記検証にて成功した場合、前記処理命令を実行するステップと、  
を有するアクセス方法。

【請求項5】

機器からメモリデバイスに対するアクセス方法であって、  
前記機器が、  
前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、  
前記可能領域情報を参照し、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、  
前記第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、  
前記メモリデバイスが、  
前記指定情報を受信するステップと、  
前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、  
前記検証にて成功した場合、前記処理命令を実行するステップと、  
を有するアクセス方法。

【請求項6】

機器からメモリデバイスに対するアクセス方法であって、  
前記機器が、  
前記メモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、  
第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、  
前記第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、  
前記メモリデバイスが、  
前記指定情報を受信するステップと、  
前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、  
前記検証にて成功した場合、前記処理命令を実行するステップと、  
を有するアクセス方法。

【請求項7】

機器からメモリデバイスに対するアクセス方法であって、  
前記メモリデバイスは、  
前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性の第2領域と、前記機器からアクセスすることが可能な第3領域と、を有し、  
少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、  
前記機器は、  
前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、

前記可能領域情報を参照し、第二の処理系コマンドを用いて、前記第2領域へのアクセス領域を指定する指定情報を送信するステップと、  
第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、  
前記メモリデバイスは、  
前記指定情報を受信するステップと、  
前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、  
前記検証にて成功した場合、前記処理命令を実行するステップと、  
を有するアクセス方法。

**【請求項8】**

機器からメモリデバイスに対するアクセス方法であって、  
前記メモリデバイスは、  
前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性の第2領域と、前記機器からアクセスすることが可能な第3領域と、を有し、  
少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、  
前記機器は、  
前記メモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、  
第二の処理系コマンドを用いて、前記第2領域へのアクセス領域を指定する指定情報を送信するステップと、  
第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、  
前記メモリデバイスは、  
前記指定情報を受信するステップと、  
前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、  
前記検証にて成功した場合、前記処理命令を実行するステップと、  
を有するアクセス方法。

**【請求項9】**

機器から読み書きされるメモリデバイスであって、  
アクセスする領域を指定する指定情報を受信するとともに、前記指定情報に基づく検証情報と読み出し又は書き込み命令を併せて受信する処理命令受信手段と、  
前記指定情報を、前記検証情報を用いて検証処理を行う指定情報検証手段と、  
データを格納する記憶領域と、  
前記検証処理が成功した場合に、前記処理命令に応じて、前記記憶領域の前記指定領域に対する読み出し又は書き込みを行う記憶領域アクセス手段と、  
前記記憶領域アクセス手段が読み出したデータを前記機器に送信するデータ送信手段と

前記機器から書き込みデータを受信するデータ受信手段と、  
を備えることを特徴とするメモリデバイス。

**【請求項10】**

前記指定情報検証手段の検証処理が、前記検証情報と検証用鍵を用いて行うことを特徴とする請求項9記載のメモリデバイス。

**【請求項11】**

前記機器との間で前記検証用鍵を共有する検証用鍵共有手段をさらに備えることを特徴とする請求項10記載のメモリデバイス。

**【請求項12】**

前記機器との間でメモリデバイスへのアクセス可能な領域を示す可能領域情報を共有する可能領域情報共有手段をさらに備えることを特徴とする請求項 9 記載のメモリデバイス。

【請求項 13】

メモリデバイスを読み書きする情報機器であって、  
読み出し又は書き込みする領域を決定し、前記領域を指定する指定情報を決定する指定情報決定手段と、

前記指定情報から前記検証情報の生成処理を行う検証情報生成手段と、

前記指定情報の送信と、前記検証情報と読み出し又は書き込みの処理命令とを併せて送信する処理命令送信手段と、

前記処理命令が書き込みの場合は、前記メモリデバイスにデータを送信するデータ送信手段と、

前記処理命令が読み出しの場合は、前記メモリデバイスからデータを受信するデータ受信手段と、

前記メモリデバイスに送信するデータを記憶し、または、前記メモリデバイスから受信したデータを記憶するデータ記憶手段と、

を備えることを特徴とする情報機器。

【請求項 14】

前記検証情報生成手段の前記検証情報の生成処理が、前記指定情報と検証用鍵とを用いて行うことを特徴とする請求項 13 記載の情報機器。

【請求項 15】

前記メモリデバイスとの間で前記検証用鍵を共有する検証用鍵共有手段を備えることを特徴とする請求項 14 記載の情報機器。

【請求項 16】

前記メモリデバイスとの間で、当該メモリデバイスへのアクセス可能な領域を示す可能領域情報を共有する可能領域情報共有手段をさらに備えることを特徴とする請求項 13 記載の情報機器。

【請求項 17】

機器からメモリデバイスに対するアクセス方法であって、

前記機器が、

前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、

前記アクセス領域への処理命令と、前記指定情報に関する検証情報を検証用鍵で暗号化した検証データと、を併せて送信するステップと、

前記メモリデバイスが、

前記指定情報を受信するステップと、

前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと検証用鍵とを用いて検証するステップと、

前記検証に成功した場合、前記処理命令を実行するステップと、

を有するアクセス方法。

【請求項 18】

機器からメモリデバイスに対するアクセス方法であって、

前記機器は、

第一の処理系コマンドを用いて前記メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、

第一の処理系コマンドを用いて前記アクセス可能領域に対応した検証用鍵を共有化するステップと、

第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、

第二の処理系コマンドを用いて前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、

前記メモリデバイスは、  
前記指定情報を受信するステップと、  
前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、  
前記検証にて成功した場合は、前記処理命令を実行するステップと、  
を有するアクセス方法。

【請求項19】

機器からメモリデバイスに対するアクセス方法であって、  
前記メモリデバイスは、  
前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性かつ大容量の第2領域と、前記機器からアクセスすることが可能なく大容量の第3領域と、を有し、  
少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、  
前記機器は、  
前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、  
第一の処理系コマンドを用いて、前記アクセス可能領域に対応した検証用鍵を共有化するステップと、  
第二の処理系コマンドを用いて、前記第2領域へのアクセス領域を指定する指定情報を送信するステップと、  
第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、  
前記メモリデバイスは、  
前記指定情報を受信するステップと、  
前記処理命令と前記検証データを受信し前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、  
前記検証にて成功した場合は、前記処理命令を実行するステップと、  
を有するアクセス方法。

## 【書類名】明細書

## 【発明の名称】アクセス方法

## 【技術分野】

## 【0001】

本発明は、PCや携帯電話などの端末に挿入して使用されるメモリカード、並びにメモリカードに対するアクセス方法に関するものである。

## 【背景技術】

## 【0002】

従来、メモリカードは端末に挿入され、端末がデータを格納するためのものである。以下に、従来のメモリカードの一例をあげる（例えば、下記特許文献1参照）。

## 【0003】

カードは、端末から各種コマンドを受け付け、またコマンドに対するレスポンスを返すコマンド用端子（CMDライン）と、データの入力を受け付け、またデータの出力を行うデータ用端子（DATライン）を持つ。

## 【0004】

図46に示した従来のメモリカードの例では、端子4602がCMDラインとなっており、端子4607、4608、4609がDATラインであり、それぞれDAT0、DAT1、DAT2となっている。また端子4601はデータ入出力用とカード検出用（CD）を兼ねたCD/DAT3となっている。DAT0～DAT3については、DAT0のみを使うモードと、DAT0～3を同時に利用しDAT0のみを使う場合の4倍の転送速度を実現するモードが存在する。

## 【0005】

次に、図47を用いて、従来カードのカード内モジュール構成について説明する。

## 【0006】

カード内モジュールは、CMDライン4602に接続された、コマンド受信及びレスポンス送信を行う処理命令受信手段4701と、DATライン4607、4608、4609、4601に接続された、データ送受信を行うデータ送受信手段4702と、記憶領域4704と、受信したコマンドに応じて記憶領域4704へのデータの読み書きを行う記憶領域アクセス手段4703からなる。

## 【0007】

次に、従来のメモリカードにおける、データ読み出し時の処理動作について説明する。ここではデータの出力はDAT0端子4607のみを利用するモードに設定されているものとするが、DAT1端子4608、DAT2端子4609、DAT3端子4601を併用するモードであってもよい。

## 【0008】

まず、端末はカードのCMDライン4602にデータ読み出しコマンドを送信する。この読み出しコマンドは図7で示されるフォーマットとなっており、6ビットのコマンドコード401と32ビットのコマンド引数402から構成される。データ読み出しコマンドにおけるコマンド引数は、読み出し開始アドレスを格納する。

## 【0009】

端末からコマンドを受信した処理命令受信手段4701は、コマンドコード401を参照して、データ読み出しコマンドであることを認識する。

## 【0010】

次に、処理命令受信手段4701は、コマンド引数402を参照して、指定されたアドレスが正しいものであるか、つまりカードが対応している範囲に指定されたアドレスが収まっているかを調べ、アドレスが正しくなければレスポンスとしてエラーである旨のレスポンスコードを返す。アドレスが正しければ正常である旨のレスポンスコードを返す。

## 【0011】

処理命令受信手段4701は、レスポンスを端末に返送した後、記憶領域アクセス手段4703に対し、指定されたアドレスとともに、読み出し要求を行う。



## 【0012】

記憶領域アクセス手段4703は、記憶領域4704の指定アドレスからデータを読み出し、データ送受信手段4702に送信する。

## 【0013】

データ送受信手段4702は、DAT0ライン4607を通じて、端末に読み出しデータの出力を行う。

## 【0014】

このようなメモリカードでは、端末からアドレスを指定して自由にカードの読み書きが可能である。

【特許文献1】特開2003-91704号公報

## 【発明の開示】

## 【発明が解決しようとする課題】

## 【0015】

上記のようなメモリカードにおいて、フラッシュメモリの特定領域をセキュリティ保護領域としてアクセス制限をかけ、アクセスが許可された特定の端末からのみアクセス可能としたい場合に、上記文献で示されたカードでは、ICカードコマンドを用いて柔軟な認証を行うことが可能である。しかし、ICカードの標準的なコマンドフォーマットであるAPDU (Application protocol data unit) では、256バイトのデータ送受信しか行えないことと、半二重プロトコルのために、ホストからのコマンド送信の度にレスポンス受信が必要であるという理由から、高速なデータ転送が困難である。そこで、ICカードコマンドを用いて、セキュリティポリシーに柔軟にあわせた方式にて認証処理を行った後でメモリカードコマンドを用いてデータ転送を行う方式が考えられるが、ICカードコマンドの発行者とメモリカードコマンドを発行したホスト上のアプリケーションが同一であることを確認することが困難である。

## 【0016】

そこで、ICカードコマンドを用いた認証処理の過程で生成した情報を、ICカードコマンドとメモリカードコマンドの発行者の同一性を検証するための検証データとしてメモリカードコマンドに含める場合、コマンド引数にアクセス領域指定情報（アクセスするアドレスなど）と認証用の検証データを含めることになるが、データ読み出しコマンドのコマンド引数402のサイズは上述の通り、32ビットの固定であるので、セキュリティを向上させるため認証用の検証データのサイズを大きくすると、アクセス領域指定情報の長さが短くなりアクセス可能な領域が制限されてしまう。一方、検証データのサイズを小さくすれば、セキュリティ強度が下がってしまう。

## 【0017】

この課題を解決するために、従来のデータ読み出しコマンドのフォーマットを変更すると、従来のメモリカードにアクセスができなくなってしまうおそれがある。

## 【0018】

また、従来のデータ読み出しコマンドと、セキュリティ保護領域を備えたメモリカードへのデータ読み出しコマンドとを別個のものとして併存させるとすると、端末側でメモリカードの種類によってコマンドを切り換える必要が発生し、メモリカードへのアクセスが複雑となり、端末にとっては利用しづらいものとなる。そのため、検証データを送信するためのコマンドとデータの読み出しまたは書き込みを行うためのメモリカードコマンドをそれぞれ定義し、2つのコマンドを組み合わせることでセキュリティ保護領域へのアクセスを行う必要があるが、2つのコマンドの間でコマンド発行者の同一性を確認することができない。

## 【0019】

そこで本発明では、メモリカード内でアクセス制限がされていない領域にアクセスする場合は、上述のデータ読み出しコマンドに代表されるメモリカードコマンドを用い、アクセス制限がされているセキュリティ保護領域に関しては、まずアクセス領域を指定するメモリカードコマンドによってアクセス領域指定情報をメモリカードに送付した後に、ホス

トとメモリカード間でICカードコマンドを用いた柔軟な認証処理を用いて共有した、または、予め共有している鍵情報と、上記アクセス領域指定情報を用いて生成した認証用の検証データを含ませた、セキュリティ保護領域の読み出しまたは書き込み用メモリカードコマンドをメモリカードに送付して、セキュリティ保護領域へのデータの書き込み、セキュリティ保護領域からのデータを読み出しする、という2段階のコマンド構成にすることで、メモリカードコマンドのフォーマットの変更を必要とせず、また少ないコマンド回数でもセキュリティを低下させることなく、セキュリティ保護領域へのアクセスを可能にするアクセス方法を提供することを目的とする。

【課題を解決するための手段】

【0020】

第1の発明は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0021】

この発明によれば、アクセス領域指定とセキュリティ保護領域アクセスのコマンドを分離し、セキュリティ保護領域アクセス用のコマンドに検証データを含めることで、アクセス領域指定を行った機器アプリケーションとセキュリティ保護領域アクセス用コマンドを発行した機器アプリケーションとメモリカードとの間で共有している検証用鍵を保持した、つまりセキュリティ保護領域にアクセスする権限を持った機器アプリケーションが同一であることをメモリデバイスが検証することが可能となる。さらに、アクセス領域指定とセキュリティ保護領域アクセスのコマンドの2段階の構成にしたことで、メモリアクセスについては従来のメモリカードコマンドを使用することでコマンドの複雑さを回避しながら、少ないコマンド回数でもセキュリティを低下させることなくセキュリティ保護領域へアクセスすることが可能になる。

【0022】

第2の発明は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0023】

この発明によれば、セキュリティ保護領域内の各領域に対して、セキュリティ保護領域アクセスコマンドによるアクセスの可否を明示的に設定することができる。

【0024】

第3の発明は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、検証用鍵を共有化するステップと、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0025】

この発明によれば、検証用鍵を必要に応じて更新することで、セキュリティ強度を向上

させることができる。

【0026】

第4の発明は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記メモリデバイスとで、前記アクセス可能領域に対応した検証用鍵を共有化するステップと、前記可能領域情報を参照し、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0027】

この発明によれば、該機器のみが読み書き可能な領域に対して、アクセスしないときはセキュリティ保護領域アクセスコマンドによるアクセスを無効化することができ、セキュリティ強度を向上することができ、検証用鍵を必要に応じて更新することで、セキュリティ強度を向上させることができる。

【0028】

第5の発明は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0029】

この発明によれば、アクセス可能な領域に関する情報の共有を、アクセス領域指定とセキュリティ保護領域アクセスのコマンドと異なるコマンド処理系で分離することが可能となり、アクセス領域指定を行った機器アプリケーションとセキュリティ保護領域アクセス用コマンドを発行した機器アプリケーションと、セキュリティ保護領域にアクセスする権限を持った機器アプリケーションが同一であることをメモリデバイスが検証することが可能となる。

【0030】

第6の発明は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

【0031】

この発明によれば、検証鍵の共有処理をセキュリティ保護領域アクセスのコマンドと異なるコマンド処理系で分離することが可能となり、その領域に限定した検証用鍵を更新することで、よりセキュリティ強度を向上することができる。

【0032】

第7の発明は、機器からメモリデバイスに対するアクセス方法であって、前記メモリデ

バースは、前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性の第2領域と、前記機器からアクセスすることが可能な第3領域と、を有し、少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、第二の処理系コマンドを用いて、前記第2領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

#### 【0033】

この発明によれば、非耐タンパである領域へのアクセスに必要なアクセス可能化設定は耐タンパ性領域の裁量で行い、データの読み書きは非タンパ性領域に適したコマンドを用いることで、セキュリティの柔軟性と読み書きのパフォーマンスを両立することができる。

#### 【0034】

第8の発明は、機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性の第2領域と、前記機器からアクセスすることが可能な第3領域と、を有し、少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記第2領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

#### 【0035】

この発明によれば、非耐タンパである領域へのアクセスに必要なアクセス可能化設定と検証用鍵共有は耐タンパ性領域の裁量で行い、データの読み書きは非タンパ性領域に適したコマンドを用いることで、セキュリティの柔軟性と読み書きのパフォーマンスを両立することができる。

#### 【0036】

第9の発明は、機器から読み書きされるメモリデバイスであって、アクセスする領域を指定する指定情報を受信するとともに、前記指定情報に基づく検証情報と読み出し又は書き込み命令を併せて受信する処理命令受信手段と、前記指定情報を、前記検証情報を用いて検証処理を行う指定情報検証手段と、データを格納する記憶領域と、前記検証処理が成功した場合に、前記処理命令に応じて、前記記憶領域の前記指定領域に対する読み出し又は書き込みを行う記憶領域アクセス手段と、前記記憶領域アクセス手段が読み出したデータを前記機器に送信するデータ送信手段と、前記機器から書き込みデータを受信するデータ受信手段と、を備えるメモリデバイスである。

#### 【0037】

この発明によれば、アクセス領域の指定とメモリへのアクセスのコマンドが異なる場合でも、前記2つのコマンドが同一端末から送信されたことを確認することができる。

#### 【0038】

第10の発明は、第9の発明のメモリデバイスにおいて、前記指定情報検証手段の検証処理が、前記検証情報と検証用鍵を用いて行うメモリデバイスである。

【0039】

この発明によれば、鍵を用いることで、端末との共有秘密情報を用いた端末の認証を行うことができる。

【0040】

第11の発明は、第10の発明のメモリデバイスにおいて、前記機器との間で前記検証用鍵を共有する検証用鍵共有手段をさらに備えるメモリデバイスである。

【0041】

この発明によれば、検証用鍵を必要に応じて更新することで、セキュリティ強度を向上させることができる。

【0042】

第12の発明は、第9の発明のメモリデバイスにおいて、前記機器との間でメモリデバイスへのアクセス可能な領域を示す可能領域情報を共有する可能領域情報共有手段をさらに備えるメモリデバイスである。

【0043】

この発明によれば、セキュリティ保護領域内の各領域に対して、セキュリティ保護領域アクセスコマンドによるアクセスの可否を明示的に設定することができる。

【0044】

第13の発明は、メモリデバイスを読み書きする情報機器であって、読み出し又は書き込みする領域を決定し、前記領域を指定する指定情報を決定する指定情報決定手段と、前記指定情報から前記検証情報の生成処理を行う検証情報生成手段と、前記指定情報の送信と、前記検証情報と読み出し又は書き込みの処理命令とを併せて送信する処理命令送信手段と、前記処理命令が書き込みの場合は、前記メモリデバイスにデータを送信するデータ送信手段と、前記処理命令が読み出しの場合は、前記メモリデバイスからデータを受信するデータ受信手段と、前記メモリデバイスに送信するデータを記憶し、または、前記メモリデバイスから受信したデータを記憶するデータ記憶手段と、を備える情報機器である。

【0045】

この発明によれば、メモリカードのセキュリティ保護領域に格納したデータを読み書きすることができる。

【0046】

第14の発明は、第13の発明の情報機器において、前記検証情報生成手段の前記検証情報の生成処理が、前記指定情報と検証用鍵とを用いて行う情報機器である。

【0047】

この発明によれば、カードと秘密供給した鍵を用いた検証を行うことで、該情報機器以外が読み書きできない領域にデータを格納することができる。

【0048】

第15の発明は、第14の発明の情報機器において、前記メモリデバイスとの間で前記検証用鍵を共有する検証用鍵共有手段を備える情報機器である。

【0049】

この発明によれば、検証用鍵を必要に応じて更新することで、セキュリティ強度を向上させることができる。

【0050】

第16の発明は、第13の発明の情報機器において、前記メモリデバイスとの間で、当該メモリデバイスへのアクセス可能な領域を示す可能領域情報を共有する可能領域情報共有手段をさらに備える情報機器である。

【0051】

この発明によれば、該情報機器のみが読み書き可能な領域に対して、アクセスしないときはセキュリティ保護領域アクセスコマンドによるアクセスを無効化することができ、セキュリティ強度を向上することができる。

## 【0052】

第17の発明は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと検証用鍵とを用いて検証するステップと、前記検証に成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

## 【0053】

この発明によれば、機器とメモリデバイスで共有した検証用鍵を用いて検証を行うことで、アクセスする権限を持った機器のみにアクセスを許可することができる。

## 【0054】

第18の発明は、機器からメモリデバイスに対するアクセス方法であって、前記機器は、第一の処理系コマンドを用いて前記メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、第一の処理系コマンドを用いて前記アクセス可能領域に対応した検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合は、前記処理命令を実行するステップと、を有するアクセス方法である。

## 【0055】

この発明によれば、セキュリティ保護領域内の領域に対してセキュリティ保護領域アクセスコマンドによるアクセスを有効にするとともに、その領域に限定した検証用鍵を更新することで、よりセキュリティ強度を向上することができる。

## 【0056】

第19の発明は、機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性かつ大容量の第2領域と、前記機器からアクセスすることが可能な大容量の第3領域と、を有し、少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、第一の処理系コマンドを用いて、前記アクセス可能領域に対応した検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記第2領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法である。

## 【0057】

この発明によれば、非耐タンパである領域へのアクセスに必要なアクセス可能化設定と検証用鍵共有は耐タンパ性領域の載量で行い、データの読み書きは大容量領域に適したコマンドを用いることで、セキュリティの柔軟性と読み書きのパフォーマンスを両立することができる。

## 【発明の効果】

## 【0058】

本発明によれば、アクセス領域指定とセキュリティ保護領域アクセスのコマンドを分離

し、セキュリティ保護領域アクセス用のコマンドに検証データを含めることで、アクセス領域指定を行った端末アプリケーションとセキュリティ保護領域アクセス用コマンドを発行した端末アプリケーションとメモリカードとの間で共有している検証用鍵を保持した、つまりセキュリティ保護領域にアクセスする権限を持った端末アプリケーションが同一であることをカードが検証することが可能となる。さらに、アクセス領域指定とセキュリティ保護領域アクセスのコマンドの2段階の構成にしたことで、メモリアクセスについては従来のメモリカードコマンドを使用することでコマンドの複雑さを回避しながら、少ないコマンド回数でもセキュリティを低下させることなくセキュリティ保護領域へアクセスすることが可能になる。

【発明を実施するための最良の形態】

【0059】

(実施の形態1)

本発明におけるカード内モジュール構成について図1を用いて説明する。なお、カード100の端子配置は、図2に示すが、その端子構成は、図46に示したものと各端子に付した符号は異なるが、その構成は同様であるため、説明は省略する。

【0060】

カード内モジュールは、コントローラ106とフラッシュメモリ105からなる。コントローラ106は、CMDラインに接続された、コマンド受信及びレスポンス送信を行うコマンド受信部101と、DATラインに接続されたデータ送受信部102と、データ送受信部102が送受信したデータに対してセッション鍵で暗復号処理を施し、またフラッシュメモリ格納用鍵で暗復号してメモリアクセス部104とのデータ受け渡しを行う暗復号部107と、フラッシュメモリ105へのデータの読み書きを行うメモリアクセス部104と、受信したコマンドに応じて、メモリアクセス部104、セッション鍵共有部110、及びパラメータ検証部108、暗復号部107に対して処理要求を行うデータ制御部103と、端末200から受信したセキュリティ保護領域にアクセスするためのパラメータを記憶しておくパラメータ記憶部109と、パラメータが正しいことを検証するパラメータ検証部108と、端末200との間で認証用及び暗復号用のセッション鍵を交換するセッション鍵共有部110と、セッション鍵と、セッション鍵と対応付けられたセキュリティ保護領域を記憶しておくエリア・セッション鍵管理部111からなる。

【0061】

次に、本実施の形態1における端末200の構成について図3を用いて説明する。

【0062】

端末200は、カード100にメモリカードコマンドを送信するコマンド送信部204と、カード100のDATラインにデータを送信するデータ送受信手段207と、データ送受信手段207が送信するデータを暗号化し、また受信するデータを復号化する暗復号手段206と、カード100との間でセッション鍵の共有処理を行うセッション鍵共有手段202と、セキュリティ保護領域アクセスコマンドによってアクセスする領域を決定し、領域指定情報を生成する、指定情報決定手段201と、領域指定情報とセッション鍵から検証データを生成する検証データ生成部203と、送信するデータ、または受信したデータを記憶するデータ記憶手段205とを備える。

【0063】

次に、図1のカード100と図3の端末200の間で行われる処理の概要について図4を用いて説明する。

【0064】

図4において、まず、端末200とカード100の間では、カード100ICカードコマンドを用いた処理として、端末200とカード100相互間を認証するための認証処理及びセッション鍵を共有するための鍵共有処理と、端末200からカード100内メモリへのアクセス可能領域の領域番号(図中の領域No. x)を割り当てる領域番号割り当て処理とが実行される(ステップS401)。

【0065】



認証処理を行い、相互に正当性が確認された後、鍵共有処理及び領域番号割り当て処理が行われ、その結果として、端末200内とカード100内には、領域No. xにて示されるセキュリティ保護領域へのアクセスを可能にする検証用及び暗号用のセッション鍵が領域番号(領域No. x)と対応付けて保持される。

**【0066】**

次に、端末200とカード100の間では、メモリカードコマンドを用いた処理として、端末200からカード100へのアクセス領域指定コマンド送信処理(ステップS402)及びデータ転送コマンド送信処理(ステップS403)と、カード100から端末200への暗号化データ送信処理(ステップS404)とが実行される。

**【0067】**

アクセス領域指定コマンド送信処理では、アクセスしたいセキュリティ保護領域内の領域を指定するため、領域No. x、ブロックアドレス及びブロック長を設定したデータを含むアクセス領域指定コマンドが端末200からカード100へ送信される。カード100では、受信したアクセス領域指定コマンドから抽出した領域No. xに基づいてセキュリティ保護領域へのアクセス可否検証処理が実行される。

**【0068】**

また、データ転送コマンド送信処理では、端末200において領域No. x、ブロックアドレス及びブロック長と、ステップS401にてカード100との間で共有した検証用鍵を用いて検証データが作成され、この検証データを含むデータ転送(Read)コマンドがカード100に送信される。カード100では、受信したデータ転送(Read)コマンドから端末200との間で共有した検証用鍵を用いて領域No. x、ブロックアドレス及びブロック長を元に検証データを作成していることを確認することで、ステップS402にて指定されたセキュリティ保護領域へのアクセス可否が検証される。

**【0069】**

また、暗号化データ送信処理では、カード100において上記検証処理においてアクセス可となった領域No. xに格納されたデータが、端末200との間で共有した暗号用鍵を用いて暗号化され、この暗号化データが端末200に送信される。

**【0070】**

以下の説明では、上記処理概要に処理手順について詳細に説明する。

**【0071】**

端末200とセッション鍵共有部110との間で送受信されるコマンド形態は、一般的なICカードで用いられるAPDUフォーマットに従った形とする。つまり、セッション鍵共有部110はICカードアプリケーションの形態をとる。

**【0072】**

ここでは、APDUの送受信方法について、図5のシーケンス図を用いて説明する。

**【0073】**

まず、端末200からカード100に対するコマンドAPDUの送信処理について説明する。ここで、コマンドAPDUとは、メモリカード側で実行させたいコマンドをAPDUフォーマット形式で端末200からメモリカード送付するものをいい、具体的にはICカード用コマンドを使用する。

**【0074】**

まず、端末200はセッション鍵共有部110に対して送信するコマンドAPDUを作成する。次に、端末200は図2のカード100のCMDライン22に対して、APDU送信コマンドを送信する(ステップS501)。

**【0075】**

このAPDU送信コマンドは、従来のデータ読み出しコマンドと同様、図7で示されるフォーマットとなっており、6ビットのコマンドコード401と32ビットのコマンド引数402から構成される。

**【0076】**

APDU送信コマンドにおけるコマンド引数402は、図16で示すように、DAT0



ライン27に入力するデータがコマンドAPDUであることを示すフラグ1401と送信データ数を示す1403とからなる。フラグ1401及び送信データ数1403を合わせて32ビットに満たない場合は未使用フィールド1402が存在する。

**【0077】**

図2のDAT0ライン27に入力するデータは512バイト単位となっており、送信データ数1403は、この512バイト単位の入力を何回行うかを示す。

**【0078】**

次に、カード100のコマンド受信部101は、端末200から送信されたコマンドを受信し（ステップS502）、それがAPDU送信コマンドであることを認識し、CMDライン22を介して端末200にレスポンスを返すとともに（ステップS503）、データ制御部103に対して、APDU送信コマンドを受信したことを通知する（ステップS504）。

**【0079】**

次に、端末200はカード100のCMDライン22からAPDU送信コマンドに対するレスポンスを受信し（ステップS503）、DAT0ライン27に図18で示すフォーマットでコマンドAPDU1602を入力する（ステップS505）。

**【0080】**

図18において、1601で示される長さは後に続くAPDU1602の長さを示している。長さフィールド1601とAPDU1602の合計長にあわせてコマンド引数の送信データ数1403が設定されている。また、前記合計長は必ずしも512バイトの倍数になるわけではないので、512バイトの倍数になるようにパディング1603を付加する。

**【0081】**

次に、カード100内部のデータ送受信部102は、端末200からDAT0ライン27に入力されたコマンドAPDUを受信するとともに（ステップS505）、データ制御部103にコマンドAPDUを受信したことを通知する（ステップS506）。次に、データ制御部103は、データ送受信部102からコマンドAPDUを読み出し（ステップS507）、セッション鍵共有部110（ICカードアプリケーション）にコマンドAPDUを渡す（ステップS508）。

**【0082】**

次に、セッション鍵共有部110は、コマンドAPDUに記述されたとおりの処理を行い（ステップS509）、処理の結果生じたデータとステータス情報をレスポンスAPDUとしてデータ制御部103に渡す（ステップS510）。このステータス情報とは、ISO7816で定義されたステータスワードであり、正常終了したか、異常終了したかを示す2バイトの値である。次に、カード100から端末200に対するレスポンスAPDUの送信処理について、図6のシーケンス図を用いて説明する。ここでレスポンスAPDUとは、カード100が実行したコマンドAPDUの処理結果をカード100から端末200へ送信するものをいう。

**【0083】**

ここでは、前記のコマンドAPDUの送信方法で示したとおり、セッション鍵共有部110が出力したレスポンスAPDUがデータ制御部103で保持されている状態であるものとする。

**【0084】**

まず、端末200は、カード100のCMDライン22に対して、APDU受信コマンドを送信する（ステップS601）。このAPDU受信コマンドは、APDU送信コマンドと同様、図7で示される従来のデータ読み出しコマンドと同様のフォーマットとなっており、6ビットのコマンドコード401と32ビットのコマンド引数402から構成される。

**【0085】**

APDU受信コマンドにおけるコマンド引数402は、図17で示すように、未使用フ

フィールド1501と送信データ数1502とからなる。送信データ数1502が32ビットに満たない場合は未使用フィールド1501が存在する。

【0086】

図2のDAT0端子27から出力されるデータは、APDU送信コマンドにおける入力データと同様に512バイト単位となっており、送信データ数1502は512バイト単位で何回出力を行うかを示す。

【0087】

次に、カード100のコマンド受信部101は、端末200から送信されたコマンドを受信し(ステップS602)、それがAPDU受信コマンドであることを認識し、CMDライン22を介して端末200にレスポンスを返すとともに(ステップS603)、データ制御部103に対して、APDU受信コマンドを受信したことを通知する(ステップS604)。

【0088】

次に、データ制御部103は、データ送受信部102に対して、セッション鍵共有部110から受け取ったレスポンスAPDUを渡す(ステップS605)。

【0089】

次に、端末200は、カード100のCMDライン22からAPDU受信コマンドに対するレスポンスを受信し(ステップS603)、DAT0ライン27を介してデータ送受信部102からレスポンスAPDUを読み出す(ステップS606)。読み出されるレスポンスAPDUは、図18で示すフォーマットで出力される。各フィールドの詳細については、APDU送信コマンドにおける入力時と同様であるため、説明を省略する。

【0090】

カード100に搭載されるフラッシュメモリ105は、図8に示すように、少なくとも端末200から従来の読み出し用コマンド及び書き込み用コマンドに代表されるメモリカードコマンドでアクセスすることが可能な通常領域(非耐タンパ性のメモリ領域)62と、前記の従来のコマンドではアクセスすることができないセキュリティ保護領域(耐タンパ性のメモリ領域)61を持つ。また、カード100は、図8に示すように、ICカードコマンドでアクセスすることが可能な耐タンパ領域(TRM: tamper resistant module)80を持つ。

【0091】

セキュリティ保護領域61は、通常、カードアプリケーションからのみアクセス可能な状態であって、端末200からの従来の読み出し用コマンド及び書き込み用コマンドに対しては、コマンド受信部101によってアクセスは排除される。

【0092】

本発明におけるメモリカードは内部に複数のカードアプリケーションを搭載することが可能となっており、図9に示すように、セキュリティ保護領域61は各アプリケーションに対して個別の領域(AP1用領域71~AP3用領域73)を割り当てることが可能である。

【0093】

セキュリティ保護領域61は、データ制御部103が管理する格納用暗号鍵(Ks)で暗号化されている。この暗号鍵は、セキュリティ保護領域61全体で1つのKsであってもよいし、各アプリケーション用のAP1用領域71~AP3用領域73に個別に格納用暗号鍵Ks\_\_1~Ks\_\_3を用意してもよい。本実施の形態では各アプリケーションAP1~3に格納用暗号鍵Ks\_\_1~Ks\_\_3を用意する。

【0094】

次に、セキュリティ保護領域61内の各アプリケーション用のAP1用領域71~AP3用領域73の内部構成について、図10を用いて説明する。

【0095】

ここでは、例としてカードアプリケーションAP1用領域71をあげている。AP1用領域71の内部はディレクトリDIR1、DIR2とファイルFILE1~FILE3を

用いた階層構造を用いたデータ管理となっている。

【0096】

カードアプリケーションAP1は、AP1用領域71内でディレクトリ移動を行い、目的のファイルが存在するディレクトリDIR1、DIR2上でファイルFILE1～FILE3に対する読み書きを行う。

【0097】

例えば、カードアプリケーションAP1がファイルFILE3にアクセスする場合は、ディレクトリDIR1に移動し、次にディレクトリDIR2に移動した後、ファイルFILE3の読み書きを行う。また、各ディレクトリDIR1、DIR2において、その下位のディレクトリまたはファイルの作成及び削除が可能である。

【0098】

次に、カード100内のセッション鍵共有部110と、端末200との間で行われるセッション鍵共有手順について図11～図14を用いて説明する。

【0099】

カードアプリケーションと端末200はそれぞれ公開鍵暗号で用いられる公開鍵と秘密鍵の対を保持し、お互いに相手の公開鍵を保持している。

【0100】

セッション鍵共有手順におけるコマンド形態は前記で示したAPDUを用いる。以降の説明においてはコマンド形態に関する記述を行わず、単にコマンドAPDU、レスポンスAPDUと表記する。

【0101】

まず、端末200は、SELECTコマンドAPDUを送信することで、カードアプリケーションAP1の選択を行う(ステップ901)。SELECTコマンドAPDUとは、以降のICカードコマンド(コマンドAPDU)をカード100内部のどのアプリケーションに送信するかを指定するコマンドAPDUであり、他のコマンドAPDUと同様にAPDU送信コマンドを用いて送信する。

【0102】

カード100は、端末200から指定されたカードアプリケーションAP1の選択が正常に完了すれば正常完了のレスポンスAPDU、完了しなければ異常終了のレスポンスAPDUを返す(ステップ902)。

【0103】

次に、端末200は、処理903を実行する。この処理903について簡単に説明すると、選択したカードアプリケーションAP1にアクセスすることを可能にするDATA2を生成するための処理である。この処理903の詳細については、図12のフローチャートを参照して説明する。

【0104】

端末200は、乱数Rhの生成を行い(ステップS9031)、乱数Rhと、端末200がアクセスしたい図10で示したファイルFILE3のファイル名を結合し、カードアプリケーションAP1が保持する秘密鍵PriSに対応した公開鍵PubSで暗号化してDATA1を生成し(ステップS9032)、さらに端末200が保持する秘密鍵PriHに対応した公開鍵PubHを示す識別子Info\_PubHとDATA1を結合してDATA2を生成する(ステップS9033)。

【0105】

図11に戻り、次に、端末200は、カードアプリケーションとのセッション鍵の共有及び、端末200がアクセス可能な領域情報の共有を行うために、ステップS9033で生成したDATA2を含んだREQ\_AREA\_INFOコマンドをカードアプリケーションに送信する(ステップ904)。

【0106】

REQ\_AREA\_INFOコマンドを受信したカードアプリケーションAP1は、処理905を実行する。この処理905の詳細については、図13のフローチャートを参照

して説明する。

【0107】

カードアプリケーションAP1は、DATA2よりDATA1を抽出し、カードアプリケーションAP1が保持する秘密鍵PriSで復号化し、乱数Rhとファイル名FILE3を得る(ステップS9051)。

【0108】

次に、DATA2より公開鍵を識別して識別子Info\_PubHを抽出し、Info\_PubHが示す公開鍵PubHに対応付けられた端末200によるアクセスが認められているかを、ファイルFILE3のアクセス権限設定を参照して確認する。権限がなければ、その旨のエラーをレスポンスAPDUとして端末200に返す。アクセスする権限があれば、FILE3のファイルサイズSIZE3を取得する(ステップS9052)。

【0109】

次に、乱数Rsを生成し(ステップS9053)、ファイルFILE3に対する端末200からのセキュリティ保護領域アクセスコマンドによるアクセスが可能となるように、図45で示すアクセス有効テーブル4500への登録を行い、端末200がセキュリティ保護領域アクセスコマンドを用いてアクセスするときに使用するためのエリア番号XをファイルFILE3に割り当て、ファイルサイズSIZE3とともにエリア・セッション鍵管理部111に記憶する(ステップS9054)。このエリア番号とは、端末200がセキュリティ保護領域アクセスコマンドによるアクセスを行うときに、アクセス領域指定コマンドによって送信するアクセス領域指定情報に含める情報をいう。

【0110】

次に、乱数Rs、エリア番号X、ファイルサイズSIZE3を結合し、DATA3を生成し(ステップS9055)、DATA3を端末200の公開鍵PubHで暗号化してDATA4を生成する(ステップS9056)。

【0111】

次に、乱数Rsと乱数Rhに排他的論理和を施し、乱数Rを生成し(ステップS9057)、乱数Rから暗号用セッション鍵Kd、検証用セッション鍵Kmを生成する(ステップS9058)。

【0112】

次に、セッション鍵Kd及びKmをエリア番号Xと関連付け、エリア・セッション鍵管理部111に記憶する(ステップS9059)。

【0113】

図11に戻り、カード100はここまでの処理を終えると端末200にDATA4を含んだレスポンスAPDUを端末200に送信する(ステップ906)。

【0114】

レスポンスAPDUを受信した端末200は、レスポンスAPDUからDATA4を抽出し、処理907を実行する。この処理907の詳細については、図14のフローチャートを参照して説明する。

【0115】

端末200は、端末200の秘密鍵PriHを用いてDATA4を復号しDATA3を取得する(ステップS9071)。次に、端末200は、DATA3より乱数Rsを取得し、乱数Rsと乱数Rhに排他的論理和を施し、乱数Rを生成し(ステップS9072)、乱数Rから暗号用セッション鍵Kd、検証用セッション鍵Kmを生成する(ステップS9073)。

【0116】

以上のステップ901から907を踏むことで、端末200とカード100間の相互認証を行い、かつ端末200が指定したファイルに対するアクセス権限があれば端末200からのアクセスが可能な状態となり、またアクセスする際に必要なエリア番号、エリア番号に割り当てられたファイルのサイズSIZE3、および検証用セッション鍵Km、暗号用セッション鍵Kdを共有することができる。

## 【0117】

なお、ステップ904において端末200からカード100に伝えられるファイル名は、カードアプリケーションが管理するファイルを直接示すものである必要はなく、カードアプリケーションがどのファイルを指しているかが認識できる形であればよい。

## 【0118】

また、端末200がアクセスしたいファイル及びステップS9054において、そのファイルに対して端末200がアクセス可能となる設定を行った際に割り当てられるエリア番号が常に同じとなるようにし、これらの情報を端末200とカード100間であらかじめ認識しておくことで、ステップ904における端末200がアクセスしたいファイル名の通知およびステップ906におけるファイルに割り当てられたエリア番号の通知を省略することもできる。

## 【0119】

さらに、本説明では、各カードアプリケーションが図10で示すようにディレクトリとファイルからなる階層構造をもち、ディレクトリ名およびファイル名でデータを管理している形態で説明したが、カードアプリケーションに割り当てられた領域を適当な大きさに分割し、分割されたそれぞれの領域に番号のような識別子を割り当てて管理する形態でもよい。その場合は、図11で示した処理手順で用いられるファイル名FILE3の代わりに前記識別子を用いる。

## 【0120】

次に、端末200からセキュリティ保護領域に対してアクセスを行う際の処理について図15及び図1を用いて説明する。図15の実線はCMDライン22、点線はDAT0ライン27における転送を表す。

## 【0121】

まず、端末200はカード100に対してメモリカードコマンドであるアクセス領域指定コマンドを送信する（ステップ1301）。このアクセス領域指定コマンドは、図7で示されるフォーマットとなっており、6ビットのコマンドコード401と32ビットのコマンド引数402から構成される。

## 【0122】

アクセス領域指定コマンドにおけるコマンド引数402は、図16で示すように、DAT0ライン27に入力するデータがアクセス領域指定情報であることを示すフラグ1401と送信データ数を示す1403とからなる。フラグ1401及び送信データ数1403を合わせて32ビットに満たない場合は未使用フィールド1402が存在する。

## 【0123】

DAT0ライン27に入力するデータは、512バイト単位となっており、送信データ数1403は、この512バイト単位の入力を何回行うかを示す。

## 【0124】

次に、カード100のコマンド受信部101は、端末200から送信されたコマンドを受信し、それがアクセス領域指定コマンドであることを認識し、端末にレスポンスを返すとともにデータ制御部103に対して、アクセス領域指定コマンドを受信したことを通知する（ステップ1302）。

## 【0125】

次に、端末200はカード100のCMDライン22からアクセス領域指定コマンドに対するレスポンスを受信し、DAT0ライン27に図19で示すフォーマットでアクセス領域指定情報1702を入力する（ステップ1303）。

## 【0126】

図19の1701で示される長さは、後に続くアクセス領域指定情報1702の長さを示している。長さフィールド1701とアクセス領域指定情報1702の合計長に合わせてコマンド引数402の送信データ数1403が設定されている。また、前記合計長は必ずしも512バイトの倍数になるわけではないので、512バイトの倍数になるようにパディング1703を付加する。

## 【0127】

アクセス領域指定情報1702は、図20で示されるように、図11のステップ906でカードから通知されたエリア番号Xを指定するエリア番号1801と、0以上であり、同じくカードから通知されたファイルサイズSIZE3の範囲で選択可能なアクセス開始アドレス1802と、1以上であり、(ファイルサイズSIZE3-アクセス開始アドレス1802)の範囲で選択可能なアクセスデータサイズ1803とで構成される。

## 【0128】

次に、カード内部のデータ送受信部102は、端末から入力されたアクセス領域指定情報1702を受信するとともに、データ制御部103にアクセス領域指定情報1702を受信したことを通知する。

## 【0129】

次に、データ制御部103は、データ送受信部102からアクセス領域指定情報1702を読み出し、エリア番号1801が、図13のステップS9054にて割り当てられたエリア番号Xであるか、アクセス開始アドレス及びアクセスデータサイズは、エリア番号Xに対応したファイルのファイルサイズ範囲に収まっているかをチェックし、異常があればカード内部に保持するエラーフラグをONに設定する。

## 【0130】

データ制御部103は、異常がなければ、図1に示すパラメータ記憶部109にアクセス領域指定情報1702(具体的にはエリア番号1801、アクセス開始アドレス1802、アクセスデータサイズ1803)を記憶する。

## 【0131】

以上が、アクセス領域を指定する処理である。

## 【0132】

次に、図8のセキュリティ保護領域61に対して読み出しを行う際の処理について説明する。

## 【0133】

図15において、端末200は、カード100に対してセキュリティ保護領域読み出しコマンドを送信する(ステップ1304)。このセキュリティ保護領域読み出しコマンドは、図6で示されるフォーマットとなっており、6ビットのコマンドコード401と32ビットのコマンド引数402から構成される。

## 【0134】

セキュリティ保護領域読み出しコマンドにおけるコマンド引数402は、セキュリティ保護領域読み出しコマンドを送信した端末が、アクセス領域指定コマンドを送信した端末200と同一であるか、またセッション鍵共有手順を経てエリア番号Xが示す領域に対するアクセス権限があることを確認された端末200と同一であることを検証するための検証データからなる。

## 【0135】

この検証データの生成方法について図21を用いて説明する。

## 【0136】

アクセス領域指定情報1702は、アクセス領域指定コマンドにおいてDAT0ライン27に入力するパラメータである。検証鍵2101は、図11のステップ907で生成した検証用セッション鍵Kmである。

## 【0137】

端末200内部の検証データ生成部203は、暗号演算を行うモジュールであり、セキュリティ保護領域アクセス(読み出しまたは書き込み)コマンドに含める検証データを生成する。ここでは、DES-MACと呼ばれるMAC(Message Authentication Code)生成処理を行う。アクセス領域指定情報1702に対してパディングデータ2105を付加した2102を入力データとして、検証鍵2101を用いてDES暗号を用いたMAC生成処理を行い、MACデータを検証データ2104として作成する。

## 【0138】

パディングデータ 2105 については、端末 200 からカード 100 に対してアクセス領域指定コマンドを送信するときにアクセス領域指定情報 1702 と併せて送信してもよいし、あらかじめ端末とカードの間で取り決めをしたパディング生成ルールに基づいて生成したパディングデータを付与してもよい。

#### 【0139】

なお、本実施の形態では DES-MAC を用いて検証データを作成しているが、他のアルゴリズムを用いてもよい。さらに、用途に応じて検証アルゴリズムを選択可能としても良い。

#### 【0140】

なお、端末 200 が正当であるか認証する必要がなく、アクセス領域指定コマンドとの対応付けのみ確認したい場合は、暗号処理を用いずに、単に SHA1 (Secure Hash Algorithm 1) や MD5 (Message Digest 5) アルゴリズムを用いたハッシュデータを検証データとして用いてもよい。

#### 【0141】

端末 200 は、上記の検証データ生成処理によって 32 ビットの検証データを生成し、セキュリティ保護領域読み出しコマンドの引数として使用する。

#### 【0142】

次に、カード 100 のコマンド受信部 101 は、端末 200 から送信されたコマンドを受信し、それがセキュリティ保護領域読み出しコマンドであることを認識し、アクセス領域指定情報 1702 に関するエラーフラグが ON に設定されている場合は、レスポンスとしてエラーを返す。また、アクセス領域指定情報 1702 に関するエラーフラグが ON に設定されていない場合は、図 15 で示すように、端末に正常レスポンスを返す (ステップ 1305) とともに、データ制御部 103 に対してセキュリティ保護領域読み出しコマンドを受信したことを通知し、パラメータ検証部 108 にコマンド引数 402 として与えられた検証データ 2104 を渡す。

#### 【0143】

次に、端末 200 は、カード 100 の CMD ライン 22 からセキュリティ保護領域読み出しコマンドに対するレスポンスを受信し、DAT0 ライン 27 からデータが出力されるのを待つ。

#### 【0144】

以降にカード 100 によるセキュリティ保護領域のデータ出力処理について説明する。

#### 【0145】

カード 100 のパラメータ検証部 108 は、パラメータ記憶部 109 からアクセス領域指定コマンドによって端末 200 から与えられ、記憶しておいたアクセス領域指定情報 1702 を読み出し、アクセス領域指定情報 1702 に含まれるエリア番号 X (1801) に対応する、図 13 のステップ S9059 で記憶した検証用セッション鍵  $K_m$  をエリア・セッション鍵管理部 111 から取得する。

#### 【0146】

次に、カード 100 のパラメータ検証部 108 は、検証用セッション鍵  $K_m$  とアクセス領域指定情報 1702 を用いて、図 22 に示した検証データ生成処理を行い、検証データ 1904 を生成する。なお、検証データ生成処理については、図 21 で示した端末 200 による検証データ生成処理と同様であるので詳細な説明は省略する。

#### 【0147】

次に、カード 100 のパラメータ検証部 108 は、上記検証データ生成処理で生成した検証データ 1904 と、端末 200 からセキュリティ保護領域読み出しコマンドの引数によって与えられた検証データ 2104 を比較し、一致しなければエラーとし、データ読み出し処理に移行しない。一致した場合は、次のデータ読み出し処理に移行することをデータ制御部 103 に通知する。

#### 【0148】

次に、カード 100 のデータ制御部 103 は、パラメータ記憶部 109 からアクセス領

域指定情報1702を読み出し、その中に含まれるエリア番号Xを取得し、エリア・セッション鍵管理部111からエリア番号に対応するファイルFILE3を認識する。

【0149】

次に、カード100のデータ制御部103は、ファイルFILE3がアプリケーションAP1用の領域であることを確認し、格納用暗号鍵Ks\_1を取得する。

【0150】

次に、カード100のデータ制御部103は、アクセス領域指定情報1702からアクセス開始アドレス1802とアクセスデータサイズ1803を取得し、ファイルFILE3として管理されている領域に対して、アクセス開始アドレス1802をオフセット、アクセスデータサイズ1803を読み出しサイズとしてメモリアクセス部104にデータ読み出し要求を行う。

【0151】

次に、カード100のデータ制御部103は、暗復号部107に対して、メモリアクセス部104によって読み出されたデータを格納用暗号鍵Ks\_1で復号化するように要求する。

【0152】

次に、カード100のデータ制御部103は、暗復号部107に対して、暗復号部107によって復号化されたデータを暗号用セッション鍵Kdで暗号化するように要求する。

【0153】

次に、カード100のデータ制御部103は、データ送受信部102に対して、暗復号部107によって暗号用セッション鍵Kdで暗号化されたデータを端末200に送信するように要求する。

【0154】

上記の処理によって、カード100からセキュリティ保護領域のデータがセッション鍵Kdによって暗号化された状態で出力可能となる。

【0155】

端末200は、カード100からデータが出力可能となったことを認識し、図15に示すように、DAT0ライン27からセッション鍵Kdによって暗号化された状態のデータを取得し（ステップ1306）、端末が保持する暗号用セッション鍵Kdによってデータを復号化し、アクセス領域指定情報1702で指定した領域のデータを得る。

【0156】

次に、セキュリティ保護領域に対して書き込みを行う際の処理について、図23を参照して説明する。

【0157】

端末200からのアクセス領域指定コマンドの送信（ステップ2001）、前記コマンドに対するカード100からのレスポンス（ステップ2002）、及びアクセス領域指定情報の送信（ステップ2003）については、それぞれ図15に示したセキュリティ保護領域に対する読み出し処理におけるステップ1301～1303と同様であるので、説明を省略する。ステップ2001～ステップ2003を行った後、端末200は、カード100に対してセキュリティ保護領域書き込みコマンドを送信する（ステップ2004）。このセキュリティ保護領域書き込みコマンドは、図6で示されるフォーマットとなっており、6ビットのコマンドコード401と32ビットのコマンド引数402から構成される。

【0158】

セキュリティ保護領域読み出しコマンドにおけるコマンド引数402は、セキュリティ保護領域読み出しコマンドを送信した端末200が、アクセス領域指定コマンドを送信した端末200と同一であるか、また、セッション鍵共有手順を経てエリア番号Xが示す領域に対するアクセス権限があることを確認された端末200と同一であるかを検証するための検証データ2104からなる。

【0159】



この検証データの生成方法についてはセキュリティ保護領域読み出しコマンドと同様であるため、詳細な説明は省略する。

**【0160】**

端末200は、検証データ生成処理によって32ビットの検証データを生成し、セキュリティ保護領域書き込みコマンドの引数として使用する。

**【0161】**

次に、カード100のコマンド受信部101は、端末200から送信されたコマンドを受信し、それがセキュリティ保護領域書き込みコマンドであることを認識し、アクセス領域指定情報1702に関するエラーフラグが設定されている場合は、レスポンスとしてエラーを返す。

**【0162】**

また、アクセス領域指定情報1702に関するエラーフラグが設定されていない場合は、CMDライン22から端末200に対して正常レスポンスを返す(ステップ2005)とともに、データ制御部103に対してセキュリティ保護領域書き込みコマンドを受信したことを通知し、パラメータ検証部108にコマンド引数として与えられた検証データ1904を渡す。

**【0163】**

次に、端末200は、カード100のCMDライン22からセキュリティ保護領域書き込みコマンドに対するレスポンスを受信し、DAT0ライン27にデータの入力を行う。ここでDAT0ライン27に入力するデータは、図11のステップ907で生成した暗号用セッション鍵Kdで暗号化したものである。また、入力データサイズは、アクセス領域指定情報1702で指定したアクセスデータサイズと同一である。

**【0164】**

以降にカードによるセキュリティ保護領域へのデータ格納処理について説明する。

**【0165】**

カード100のパラメータ検証部108は、パラメータ記憶部109からアクセス領域指定コマンドによって端末200から与えられ、記憶しておいたアクセス領域指定情報1702を読み出し、アクセス領域指定情報1702に含まれるエリア番号X(1801)に対応する、図13のステップ9059で記憶した検証用セッション鍵Kmをエリア・セッション鍵管理部111から取得する。

**【0166】**

次に、カード100のパラメータ検証部108内部の検証データ生成部1903は、検証用セッション鍵Kmとアクセス領域指定情報1702を用いて、図22に示した検証データ生成処理を行い、検証データ1904を生成する。なお、検証データ生成処理については、図21で示した端末による検証データ生成処理と同様であるので詳細な説明は省略する。

**【0167】**

次に、カード100のパラメータ検証部108は、上記で生成した検証データ1904と、端末200からセキュリティ保護領域書き込みコマンドの引数によって与えられた検証データ2104を比較し、一致しなければエラーとし、データ書き込み処理に移行しない。一致した場合は次のデータ書き込み処理に移行することをデータ制御部103に通知する。

**【0168】**

次に、カード100のデータ制御部103は、パラメータ記憶部109からアクセス領域指定情報1702を読み出し、その中に含まれるエリア番号Xを取得し、エリア・セッション鍵管理部111からエリア番号に対応するファイルFILE3を認識する。

**【0169】**

次に、カード100のデータ送受信部102は、端末200から入力されたデータを受信する。

**【0170】**

次に、カード100のデータ制御部103は、ファイルFILE3がアプリケーションAP1用の領域71の中に存在することから、アプリケーションAP1用領域71に対応した格納用暗号鍵Ks\_1を取得する。

【0171】

次に、カード100のデータ制御部103は、暗復号部107に対して、データ送受信部102が受信したデータを暗号用セッション鍵Kdで復号化するように要求する。

【0172】

次に、カード100のデータ制御部103は、暗復号部107に対して、暗復号部107が復号化したデータを格納用暗号鍵Ks\_1で暗号化するように要求する。

【0173】

次に、カード100のデータ制御部103は、アクセス領域指定情報1702からアクセス開始アドレス1802とアクセスデータサイズ1803を取得し、ファイルFILE3として管理されている領域に対し、アクセス開始アドレス1802をオフセット、アクセスデータサイズ1803を書き込みサイズとして、メモリアクセス部104に対してデータ書き込み要求を行う。

【0174】

上記のようにして、端末200が入力したセッション鍵Kdで暗号化されたデータを格納鍵Ks\_1で暗号化してフラッシュメモリ105に格納する。

【0175】

本実施の形態では、セッション鍵の共有と、アクセス可能領域に関する情報の共有を1つのコマンドで同時に行っているが、別コマンドとして行ってもよい。

【0176】

本実施の形態では、図11にてセッション鍵共有手順を含めているが、セキュリティポリシーとしてセッション鍵を毎回更新する必要がないと考える場合は、端末200およびカード100があらかじめ検証鍵および暗号鍵を保持し、それをセッション鍵として用いてもよい。

【0177】

以上、本発明のように、ICカード用コマンドとメモリアクセス用コマンドを受信可能なメモリカードにおいて、カードアプリケーションが利用し、通常はカードアプリケーション経由でのみアクセス可能であり、端末からのアクセスが制限されているセキュリティ保護領域に対して、カードアプリケーションと端末が相互認証し、カードアプリケーションがアクセス可能設定を行うことにより、端末からメモリアクセス用コマンドを用いてアクセスすることが可能となる。

【0178】

また、カードアプリケーションがアクセス可能設定を行うためのカードアプリケーションと端末間の相互認証は、用途が限定されたメモリアクセス用コマンドではなく、ICカード用コマンドを使うことにより、データのセキュリティレベルに応じて相互認証方式を柔軟に選択可能となる。

【0179】

また、メモリアクセス用コマンドに含まれる引数サイズが32ビットのように小さい場合でも、本発明のように、アクセス領域指定とセキュリティ保護領域アクセスのコマンドを分離し、セキュリティ保護領域アクセス用のコマンドに検証データを含めることで、アクセス領域指定を行った端末アプリケーションとセキュリティ保護領域アクセス用コマンドを発行した端末アプリケーションと検証用鍵を保持した端末アプリケーションが同一であることをカードが検証することが可能となる。

【0180】

また、検証用及び暗号用セッション鍵の共有処理をセキュリティ保護領域アクセスのたびに行うことにより、セキュリティ保護領域アクセスに含める検証データとして適当な値を設定して繰り返し不正アクセスを行う攻撃に対する防御性を高めることができる。

【0181】

また、端末からアクセスしたいファイルをカードに通知し、それにエリア番号を割り当て、カードから端末に通知することにより、端末がアクセス可能な領域を設定することが可能となる。また、複数のファイルに対して行うことにより、同時に複数のファイルに対してアクセス可能な状態を作ることができる。

#### 【0182】

##### (実施の形態2)

本実施の形態では、端末が、領域指定コマンドで指定するエリア番号をあらかじめ認識している場合のシーケンスを説明する。

#### 【0183】

まず、カード内モジュール構成について図24を用いて説明する。なお、図24のカード500の端子構成は、図2に示したものと同様であるため、その図示及び説明は省略する。

#### 【0184】

カード500内モジュールは、CMDラインに接続され、コマンドの受信及びレスポンスの送信を行う処理命令受信手段501と、データを格納する記憶領域506と、記憶領域506へのアクセス処理を行う記憶領域アクセス手段505と、DATラインに接続され、記憶領域アクセス手段505が読み出したデータを外部機器に送信するデータ送信手段502と、同じくDATラインに接続され、外部機器からデータを受信するデータ受信手段503と、処理命令受信手段501が受け取った指定情報を検証する指定情報検証手段504と、からなる。

#### 【0185】

次に、端末600内モジュール構成について、図25を用いて説明する。

#### 【0186】

端末600内モジュールは、カード500に対するコマンド送信と、レスポンス受信を行う処理命令送信手段604と、カード500に対するデータ送信を行うデータ送信手段605と、カード500からのデータ受信を行うデータ受信手段606と、アクセスする領域を決定する指定情報決定手段601と、指定情報から検証情報を生成する検証情報生成手段602と、カード500に送信するデータ及びカード500から受信するデータを格納するデータ記憶手段603と、からなる。

#### 【0187】

次に、端末600からカード500のセキュリティ保護領域に対してアクセスを行う際の処理について、上記図24及び図25と、図26に示すフローチャートを用いて説明する。

#### 【0188】

まず、端末600は指定情報決定手段601にてリードアクセス又はライトアクセスを行う領域を決定し(ステップS2601)、アクセス領域指定情報を生成する(ステップS2602)。次に、このアクセス領域指定情報をデータ記憶手段603に格納して領域指定命令を処理命令送信手段604からカード500に送信する(ステップS2603)。

。

#### 【0189】

領域指定命令のデータ部の一例を図27に示す。

#### 【0190】

DAT0ライン27に入力するデータは512バイト単位となっており、領域指定命令のデータ部は、アクセス領域指定情報2702の長さフィールド2701と、アクセス領域指定情報フィールド2702の合計長が512バイトに満たない場合、パディング2703が追加される。本実施の携帯では、長さフィールド2701は2バイトの長さを持ち、アクセス領域指定情報2702は、図28に示すように、1バイトのエリア番号2801、3バイトのアクセス開始アドレス2802、及び3バイトのアクセスデータサイズ2803からなる。つまり合計9バイトであり512バイトに満たないため、503バイトのパディング2703が付加される。

## 【0191】

次に、図26に戻り、カード500は、処理命令受信手段501にて領域指定命令を受信すると（ステップS2604）、指定情報検証手段504にてアクセス領域指定情報2702を確認し、指定した領域が正しいかどうかをエリア番号2801に対応する領域が存在するか、アクセス開始アドレス2802及びアクセスデータサイズ2803がエリア番号2801で示された領域の範囲に収まっているかを元に判断する（ステップS2605）。指定情報検証手段504は、指定した領域が正しくなければ、領域指定命令を無効として扱う（ステップS2606）。指定した領域が正しい場合、アクセス領域指定情報2702を保存し、アクセス領域指定情報2702と、端末600とカード500の間で共有している鍵を用いて、比較情報を生成する（ステップS2607）。

## 【0192】

比較情報の生成方法の一例を図29に示す。

## 【0193】

検証データ生成部2902は暗号演算を行うモジュールであり、本実施の形態ではDES-MACと呼ばれるMAC（Message Authentication Code）を生成する処理を行う。入力は、領域指定命令のデータ部2704と、端末600との間で共有している検証用の鍵2901である。DES-MACの出力結果は64ビットであるが、本実施の形態では、比較対象となる端末600から送信される検証情報が32ビットであるため、その出力を切り詰めた2903である前半32ビットのみを比較情報2904として用いる。なお、検証用鍵2901は、エリア番号に対応して個別かつ固定の鍵であってもよいし、エリア番号によらず1つの鍵であってもよい。

## 【0194】

また、図30に示すように、カード700内部に検証用鍵共有手段701を備え、図31に示すように端末800内部に検証用鍵共有手段801を備え、カード700と端末800の間で、セキュリティ保護領域へのアクセスを行うたびに検証用鍵を変更してもよい。なお、図30及び図31の各構成において、図24及び図25に示した構成と同一部分には同一符号を付している。

## 【0195】

次に、検証用鍵の共有方法について上記図30及び図31と、図32に示すシーケンスおよび図33に示す検証用鍵生成方法を用いて説明する。

## 【0196】

図32において、端末800は検証用鍵共有手段801において、乱数Raを生成し、この乱数Raを含んだセッション鍵共有要求コマンドAPDUを作成し、処理命令送信手段604からAPDU送信コマンドをカード700に送信するとともに（ステップS3201）、データ送信手段605からセッション鍵共有要求コマンドAPDUをカード700に送信する（ステップS3202）。

## 【0197】

次に、カード700は処理命令受信手段501にてAPDU送信コマンドを端末800から受信し、データ受信手段503にて端末800から受信したセッション鍵共有要求コマンドAPDUを検証用鍵共有手段701に渡す。

## 【0198】

検証用鍵共有手段801では、乱数Rbを生成し、図33に示すように、端末800から受信した乱数Raと乱数Rbを結合したものに対し、あらかじめ端末800との間で共有しているマスター鍵Kを用いて暗号化処理（DES-MAC処理）を行い、セッション鍵Rを生成する。次に、カード700は、乱数Rbを含むレスポンスAPDUを生成する。

## 【0199】

次に、端末800は、処理命令送信手段604からAPDU受信コマンドをカード700に送信する（ステップS3203）。

## 【0200】

次に、カード700は、処理命令受信手段501にてAPDU受信コマンドを端末800から受信し、先ほど作成した乱数Rbを含むレスポンスAPDUをデータ送信手段502より端末800に送信する（ステップS3204）。

#### 【0201】

次に、端末800は、データ受信手段606によりレスポンスAPDUをカード700から受信し、検証用鍵共有手段801に渡す。検証用鍵共有手段801は、図33に示すように、先ほど自身が生成した乱数Raと、レスポンスAPDUに含まれる乱数Rbを結合したものに対し、あらかじめカード700との間で共有しているマスター鍵Kを用いて暗号化処理（DES-MAC処理）を行い、セッション鍵Rを生成する。

#### 【0202】

以上が、セキュリティ保護領域へのアクセスを行うたびにセッション鍵を変更する場合の、端末800とカード700の間における検証用鍵共有手順である。

#### 【0203】

なお、本実施の形態ではDES-MACを用いているが、当然他の暗号アルゴリズムを用いてもよい。また、端末800が正当であるか、つまり同一の鍵を持っているかを検証する必要がない場合、例えば、領域指定命令のアクセス領域指定情報2702が端末の意図したものになっているかの検証のみ行う場合は、暗号処理を用いずに、図34に示すような検証データ生成部3401にてSHA-1演算や、MD5アルゴリズムを用いたハッシュ演算やチェックサム演算の結果を比較情報として用いることができる。これらのアルゴリズムを用いた場合も、比較対象が32ビット長ならば、出力結果を切りつめ3402、その一部の32ビットのみを比較情報3403とする。

#### 【0204】

次に、図26に戻り、端末800は、検証データ生成部にてアクセス領域指定情報2702と、端末800とカード700の間で共有している検証用鍵2901から検証情報を生成する（ステップS2608）。

#### 【0205】

この検証情報の生成について、図35に示す。検証情報生成部3502にて検証用鍵3501と領域指定命令のデータ部2704を用いて暗号処理を行い、検証情報3504を生成する。生成方法は、図29で示したカード700における比較情報2904の生成方法と全く同じである。

#### 【0206】

次に、図26に戻り、端末800は、生成した検証情報3504をアクセス命令（読み出し）の引数に載せて、処理命令送信手段604からアクセス命令を送信する（ステップS2609）。

#### 【0207】

アクセス命令は、図36で示すフォーマットとなっており、コマンドコード3601とコマンド引数3602の長さはそれぞれ6ビットと32ビットである。アクセス命令では、コマンド引数3602に検証情報3504を格納する。

#### 【0208】

次に、図26に戻り、カード700は、処理命令受信手段501にてアクセス命令（読み出し）を受信し（ステップS2610）、指定情報検証手段504にて事前に領域指定命令が正常に完了したかどうかを確認する（ステップS2611）。領域指定命令が未受信である、又は指定した領域が正しくないなどの理由で正常に完了していない場合は、アクセス命令をエラーとして端末800に通知する（ステップS2612）。この時、端末800は、カード700からエラーを受信する（ステップS2612A）。

#### 【0209】

事前に領域指定命令が正常に完了している場合、指定情報検証手段504は、先ほどカード700が作成した比較情報2904と、アクセス命令のコマンド引数に格納された検証情報3504を比較する（ステップS2613）。比較の結果、検証情報3504が不正であったならば、アクセス命令をエラーとして端末800に通知する（ステップS26

14)。この時、端末800は、カード700からエラーを受信する（ステップS2614A）。検証情報が正常であったならば、指定情報検証手段504は記憶領域アクセス手段505にアクセス領域指定情報2702を通知し、記憶領域アクセス手段505は記憶領域506内のアクセス領域指定情報2702で指定された領域からデータを読み出し、データ送信手段502からデータを端末800に送信する（ステップS2615）。

#### 【0210】

次に、端末800は、カード700から送信された読み出しデータをデータ受信手段606にて受信し（ステップS2616）、データ記憶手段603に格納する。

#### 【0211】

以上の通り、メモリアクセス用コマンドに含められる引数サイズが32ビットのように小さい場合でも、本発明のように、アクセス領域指定とセキュリティ保護領域アクセスのコマンドを分離し、セキュリティ保護領域アクセス用のコマンドに検証データを含めることで、アクセス領域指定を行った端末アプリケーションとセキュリティ保護領域アクセス用コマンドを発行した端末アプリケーションと検証用鍵を保持した端末アプリケーションが同一であることをカードが検証することが可能となる。

#### 【0212】

なお、検証データ生成のために、領域指定情報と検証用鍵に加え、カードから出力される乱数情報を利用する方法を、図37に示すフローチャートを用いて以下に説明する。なお、図37に示す各ステップにおいて、図26に示したフローチャートのステップと同一のステップには同一符号を付して、その説明は省略する。

#### 【0213】

図37に示すように、端末800から乱数取得命令を端末800からカード700に送信し（ステップS3701）、カード700が乱数Tを生成し、この乱数Tをカード700内部の指定情報検証手段504に保持するとともに、データ送信手段502から端末800に送信する（ステップS3702）。端末800は、カード700から送信された乱数Tをデータ受信手段606にて受信する（ステップS3703）。

#### 【0214】

乱数Tを検証情報生成処理に利用する場合のカード700における比較情報の生成処理（ステップS2607）、および、端末800における検証情報の生成処理（ステップS2608）は、それぞれ図38および図39で示すように、乱数Tと領域指定命令のデータ部2704を結合したのに対して暗号処理を行い、比較情報3804及び検証情報3904を出力する。

#### 【0215】

以上のように、検証情報生成に乱数情報を利用することにより、同一の領域指定情報と検証用鍵を用いて検証情報を作成しても、乱数情報が変化することで出力される検証情報が変化するため、よりセキュリティ強度を向上させることができる。

#### 【0216】

##### （実施の形態3）

本実施の形態では、鍵の共有処理を含むシーケンスの例を説明する。

#### 【0217】

まず、カード内モジュール構成について図40を用いて説明する。なお、カードの端子構成は、図2に示したものと同様であるため、その図示及び説明は省略する。

#### 【0218】

カード内モジュールは、CMDラインに接続され、コマンドの受信及びレスポンスの送信を行う処理命令受信手段901と、データを格納する記憶領域906と、記憶領域906へのアクセス処理を行う記憶領域アクセス手段905と、DATラインに接続され、記憶領域アクセス手段905が読み出したデータを外部機器に送信するデータ送信手段902と、同じくDATラインに接続され、外部機器からデータを受信するデータ受信手段903と、端末1000との間でセキュリティ保護領域アクセスコマンドによるアクセスが可能な領域に関する情報を共有する可能領域情報共有部907と、データ受信手段903

經由して受け取った指定情報を、検証用鍵を用いて検証する指定情報検証手段904と、からなる。

#### 【0219】

次に、端末内モジュール構成について、図41を用いて説明する。

#### 【0220】

端末内モジュールは、カード900に対するコマンド送信と、レスポンス受信を行う処理命令送信手段1004と、カード900に対するデータ送信を行うデータ送信手段1005と、カード900からのデータ受信を行うデータ受信手段1006と、アクセスする領域を決定する指定情報決定手段1001と、セキュリティ保護領域アクセスコマンドによるアクセスが可能な領域に関する情報を共有する可能領域情報共有部1007と、指定情報から検証情報を生成する検証情報生成手段1002と、カード900に送信するデータ及びカード900から受信するデータを格納するデータ記憶手段1003と、からなる。

#### 【0221】

次に、端末1000からカード900内のセキュリティ保護領域に対してアクセスを行う際の処理について、上記図40及び図41と、図42及び図43に示すフローチャートを用いて説明する。

#### 【0222】

まず、端末1000は、指定情報決定手段1001にて、リードアクセス又はライトアクセスを行う領域Aを決定し（ステップS4201）、可能領域情報共有部1007にて、前記領域Aに対するセキュリティ保護領域アクセスコマンドによるアクセスを許可するように要求するコマンドAPDUである領域開放要求コマンドを処理命令送信手段1004からカード900に送信する（ステップS4202）。領域開放要求コマンドは、端末1000の公開鍵を表す識別子Info\_PubHと、領域Aを示す識別子aをカード900の公開鍵PubSで暗号化したデータとを含む。なお、コマンドAPDUの送信方法は実施の形態1で説明した方法と同様であるので、詳細な説明は省略する。

#### 【0223】

次に、カード900は、領域開放要求コマンドを受信すると（ステップS4203）、可能領域情報共有手段907にてコマンドに含まれる暗号化データをカード900自身の秘密鍵PriSで復号化する（ステップS4204）。次いで、端末1000の公開鍵識別子Info\_PubHからコマンドを送信した端末1000を識別し、識別子aで示される領域Aのアクセス権限を参照することで、該端末1000が領域Aに対するアクセスを許可されているかどうかを確認する（ステップS4205）。

#### 【0224】

アクセスが許可されていない場合は、領域開放失敗を示すデータをレスポンスAPDUとしてデータ送信手段902から端末1000に送信する（ステップS4206）。アクセスが許可されている場合は、領域Aの識別子aと領域Aに割り当てたエリア番号Xを、指定情報検証手段904内に持つ、セキュリティ保護領域アクセスコマンドによるアクセス可否を設定するアクセス有効テーブル4400（図44参照）に登録する（ステップS4207）。次に、領域Aに対応した検証用鍵Rをアクセス有効テーブル4400に登録する（ステップS4208）。

#### 【0225】

次に、エリア番号X、領域Aのサイズを端末1000の公開鍵PubHで暗号化し、レスポンスAPDUとしてデータ送信手段902から端末1000に送信する（ステップS4209）。

#### 【0226】

次に、端末1000は、APDU受信コマンドを処理命令送信手段1004からカード900に送信し、データ受信手段1006を用いてレスポンスAPDUをカード900から取得する（ステップS4210）。なお、レスポンスAPDUの取得方法は実施の形態1で説明した方法と同様であるので、詳細な説明は省略する。

## 【0227】

次に、端末1000の可能領域情報共有手段1007は、レスポンスAPDUに含まれる暗号データを端末1000自身の秘密鍵PriHで復号化し（ステップS4211）、エリア番号X、エリア番号Xで示される領域Aのサイズを得る。次に、端末1000は領域Aに対応したセッション鍵を検証情報生成手段1002に登録する。エリア番号Xはアクセス領域指定情報を生成するために指定情報決定手段1001に登録する（ステップS4212）。以後、図43のフローチャートに移行する。

## 【0228】

次に、端末1000は指定情報決定手段1001にて可能領域情報共有手段1007によって登録されたエリア番号Xを用いてアクセス領域指定情報を生成する（ステップS4213）。次に、このアクセス領域指定情報をデータ部2704（図27参照）に格納して、領域指定命令を処理命令送信手段1004からカード900に送信する（ステップS4214）。なお、領域指定命令におけるアクセス領域指定情報は実施の形態2と同様であるので、詳細な説明は省略する。

## 【0229】

次に、カード900は、処理命令受信手段901にて端末1000から領域指定命令を受信すると（ステップS4215）、指定情報検証手段904にてアクセス領域指定情報を確認し、エリア番号Xがアクセス有効テーブル4400に登録されているか、図28に示したアクセス開始アドレス2802及びアクセスデータサイズ2803を元に領域Aの範囲に収まっているか判断する（ステップS4216）。指定情報検証手段904は、指定した領域が正しくなければ、領域指定命令を無効として扱う（ステップS4217）。指定した領域が正しい場合、アクセス領域指定情報を保存し、アクセス領域指定情報とアクセス有効テーブル4400に登録された領域Aに対応した検証用鍵Rを用いて、比較情報を生成する（ステップS4218）。なお、比較情報の生成方法は実施の形態2と同様であるので、詳細な説明は省略する。

## 【0230】

次に、端末1000は、検証情報生成手段1002にてアクセス領域指定情報と、可能領域情報共有部1007によって登録されたセッション鍵Rを用いて検証情報を生成し（ステップS4219）、アクセス命令（読み出し）の引数に載せて、処理命令送信手段1001からアクセス命令をカード900に送信する（ステップS4220）。なお、検証情報の生成方法及びアクセス命令の送信方法は実施の形態2と同様であるので、詳細な説明は省略する。

## 【0231】

次に、カード900は、処理命令受信手段901にてアクセス命令（読み出し）を受信し（ステップS4221）、指定情報検証手段904にて事前に領域指定命令が正常に完了したかどうかを確認する（ステップS4222）。領域指定命令が未受信である、又は指定した領域が正しくないなどの理由で正常に完了していない場合は、アクセス命令をエラーとして端末1000に通知する（ステップS4223）。この時、端末1000は、カード900からエラーを受信する（ステップS4223A）。

## 【0232】

事前に領域指定命令が正常に完了している場合、指定情報検証手段904は、先ほどカード900が作成した比較情報と、アクセス命令の引数に格納された検証情報を比較する（ステップS4224）。比較の結果、検証情報が不正であったならば、アクセス命令をエラーとして端末1000に通知する（ステップS4225）。この時、端末1000は、カード900からエラーを受信する（ステップS4225A）。

## 【0233】

検証情報が正常であったならば、指定情報検証手段904は、記憶領域アクセス手段905に指定情報を通知し、記憶領域アクセス手段905は記憶領域906内の領域指定命令で指定された領域からデータを読み出し、データ送信手段902からデータを端末1000に送信する（ステップS4226）。



## 【0234】

次に、端末1000は、カード900から送信された読み出しデータをデータ受信手段1006にて受信し、データ記憶手段1003に格納する（ステップS4227）。

## 【0235】

次に、端末1000は、領域Aに対するセキュリティ保護領域アクセスコマンドによるアクセスが不要になったとき、領域Aに対応するエリア番号Xを無効化するための領域無効コマンドAPDUを作成し、データ送信手段1005からカード900に送信する（ステップS4228）。

## 【0236】

次に、領域無効コマンドAPDUを受信したカード900は、アクセス有効テーブル4400を検索し、エリア番号Xが見つければ、テーブル内のエリア番号Xに割り当てられた領域識別子a、セッション鍵Rとともにエリア番号Xの登録を削除し、エリア番号Xを指定した領域Aへのセキュリティ保護領域アクセスコマンドによるアクセスを無効化する（ステップS4229）。

## 【0237】

以上の通り、セキュリティ保護領域内のある領域に対し、必要な場合のみ領域開放要求によってセキュリティ保護領域アクセスコマンドによるアクセスが可能な状態にし、また不要となったときは領域無効要求によって、その領域へのアクセスを不可能にすることで、セキュリティ強度を向上させることができる。

## 【産業上の利用可能性】

## 【0238】

本発明にかかるアクセス方法は、メモリカードコマンドとICカードコマンドを併用し、メモリアクセスについてはメモリカードコマンドを使用することで複雑さを回避しながら、少ないコマンド引数でも安全に端末を認証可能とすることである。

## 【図面の簡単な説明】

## 【0239】

【図1】本発明の実施の形態1におけるメモリカードの内部モジュール構成を示す図

【図2】カードの端子構成を示す図

【図3】本実施の形態1における端末の内部構成を示す図

【図4】本実施の形態1におけるカードと端末の間で行われる処理の概要を示す図

【図5】本実施の形態1におけるAPDUの送受信方法のシーケンスを示す図

【図6】本実施の形態1におけるレスポンスAPDUの送信処理のシーケンスを示す図

【図7】本実施の形態1におけるメモリカードのコマンドフォーマットを示す図

【図8】本実施の形態1におけるフラッシュメモリの内部構成を示す図

【図9】本実施の形態1におけるセキュリティ保護領域の内部構成を示す図

【図10】本実施の形態1におけるセキュリティ保護領域内の各アプリケーション用領域の内部構成を示す図

【図11】本実施の形態1におけるセッション鍵共有及びアクセス可能領域共有手順を示す図

【図12】図11のステップ903における処理の詳細を説明するためのフローチャート

【図13】図11のステップ905における処理の詳細を説明するためのフローチャート

【図14】図11のステップ907における処理の詳細を説明するためのフローチャート

【図15】本実施の形態1における端末からセキュリティ保護領域を読み出すためのコマンドシーケンスを示す図

【図16】本実施の形態1におけるAPDU送信コマンドの引数フォーマットを示す図

【図17】本実施の形態1におけるAPDU受信コマンドの引数フォーマットを示す図

【図18】本実施の形態1におけるAPDU送信コマンドの入力データ及びAPDU受信コマンドの出力データのフォーマットを示す図

【図19】本実施の形態1におけるアクセス領域指定コマンドの入力データフォーマットを示す図

【図20】本実施の形態1におけるアクセス領域指定情報を示す図

【図21】本実施の形態1における端末の正当性検証を行うための検証データの端末による生成方法を示す図

【図22】本実施の形態1における端末の正当性検証を行うための検証データのカードによる生成方法を示す図

【図23】本実施の形態1における端末からセキュリティ保護領域に書き込むためのコマンドシーケンスを示す図

【図24】本発明の実施の形態2におけるメモリカードの内部モジュール構成を示す図

【図25】本実施の形態2における端末の内部構成を示す図

【図26】本実施の形態2における端末からカードのセキュリティ保護領域に対してアクセスを行う際の処理を示すフローチャート

【図27】本実施の形態2における領域指定命令のデータ部の一例を示す図

【図28】図27のアクセス領域指定情報のフォーマットを示す図

【図29】本実施の形態2における比較情報の生成方法の一例を示す図

【図30】本実施の形態2における内部に検証用鍵共有手段を備える場合のカード構成を示す図

【図31】本実施の形態2における内部に検証用鍵共有手段を備える場合の端末構成を示す図

【図32】本実施の形態2における検証用鍵の共有方法のシーケンスを示す図

【図33】本実施の形態2における検証用鍵生成方法を説明するための図

【図34】本実施の形態2におけるSHA-1演算を用いた比較情報生成方法を示す図

【図35】本実施の形態2における検証情報生成方法を示す図

【図36】本実施の形態2におけるアクセス命令のフォーマットを示す図

【図37】本実施の形態2における乱数情報を利用した検証データ生成処理を示すフローチャート

【図38】本実施の形態2における乱数を利用した比較情報生成方法を示す図

【図39】本実施の形態2における乱数を利用した検証情報生成方法を示す図

【図40】本発明の実施の形態3におけるメモリカードの内部モジュール構成を示す図

【図41】本実施の形態3における端末の内部構成を示す図

【図42】本実施の形態3における端末からカード内のセキュリティ保護領域へのアクセス処理の一部を示すフローチャート

【図43】図42に続くアクセス処理の一部を示すフローチャート

【図44】本実施の形態3におけるアクセス有効テーブルの一例を示す図

【図45】本実施の形態1におけるアクセス有効テーブルの一例を示す図

【図46】従来のメモリカードの端子構成を示す図

【図47】従来のカード内モジュール構成を示す図

#### 【符号の説明】

【0240】

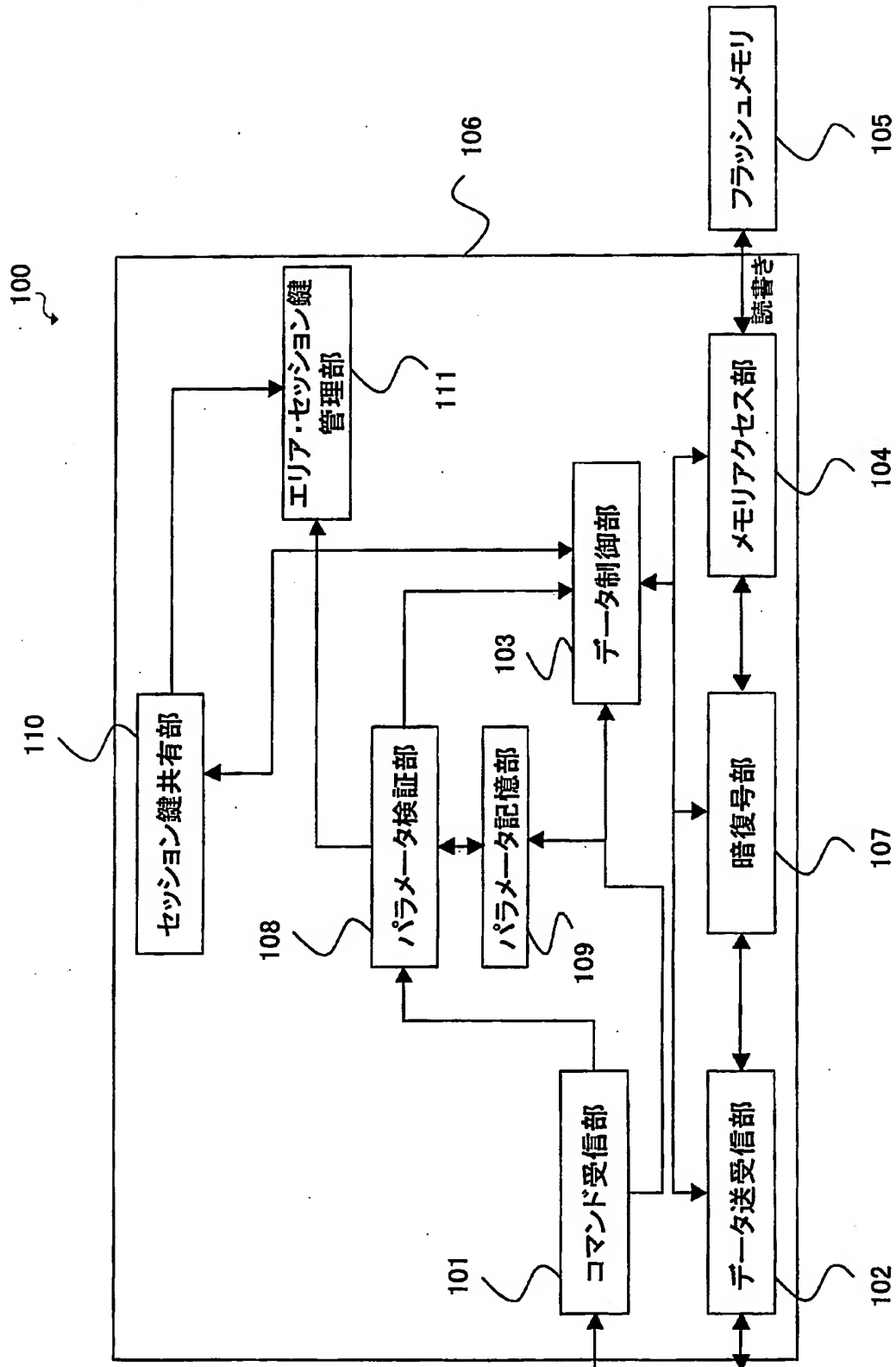
100、500、700、900 カード

200、600、800、1000 端末

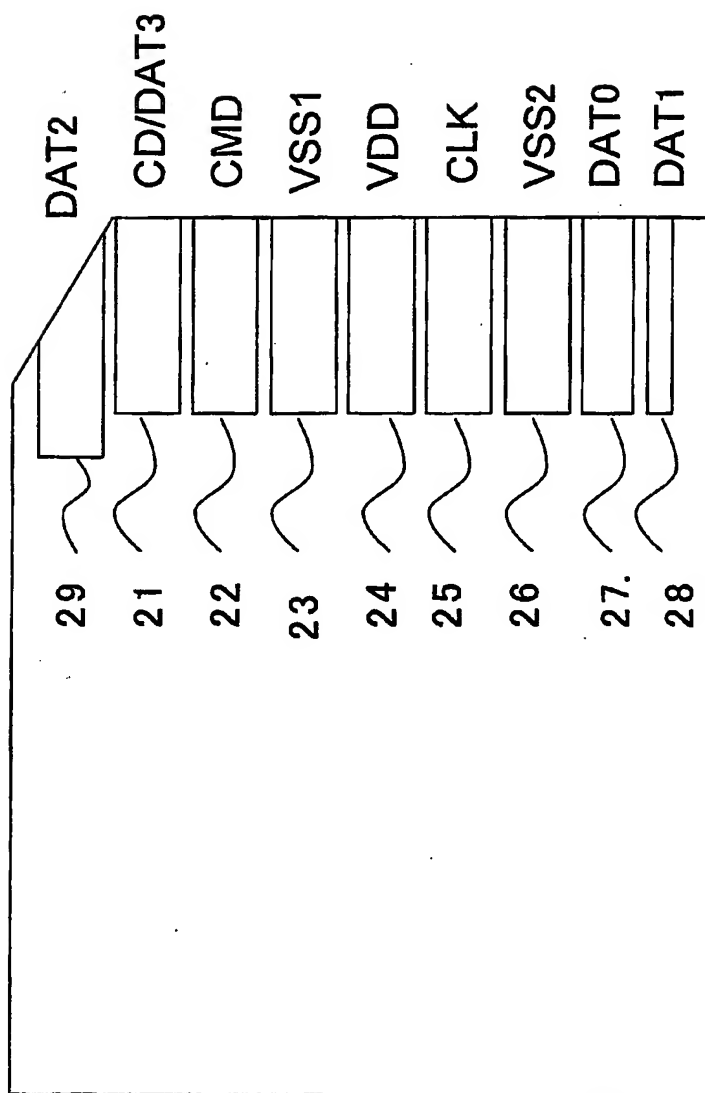
101 コマンド受信部

102 データ送受信部  
 103 データ制御部  
 104 メモリアクセス部  
 105 フラッシュメモリ  
 106 コントローラ  
 107 暗復号部  
 108 パラメータ検証部  
 109 パラメータ記憶部  
 110 セッション鍵共有部  
 111 エリア・セッション鍵管理部  
 201、601、1001 指定情報決定手段  
 202 セッション鍵共有手段  
 203 検証データ生成部  
 204 コマンド送信部  
 205、603、1003 データ記憶手段  
 データ記憶手段  
 206 暗復号手段  
 207 データ送受信手段  
 501、901 処理命令受信手段  
 502、605、902、1005 データ送信手段  
 503、606、903、1006 データ受信手段  
 504、904 指定情報検証手段  
 505、905 記憶領域アクセス手段  
 506、906 記憶領域  
 602、1002 検証情報生成手段  
 604、1004 処理命令送信手段  
 801 検証用鍵共有手段  
 907、1007 可能領域情報共有手段  
 4400、4500 アクセス有効テーブル

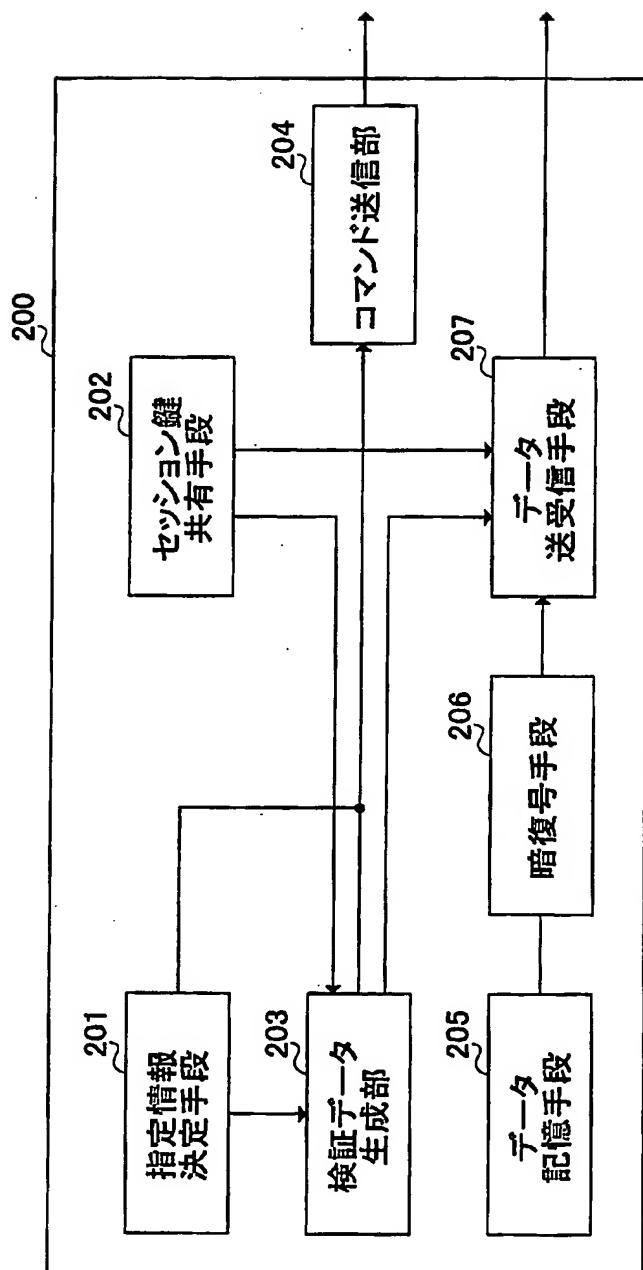
【書類名】図面  
【図1】



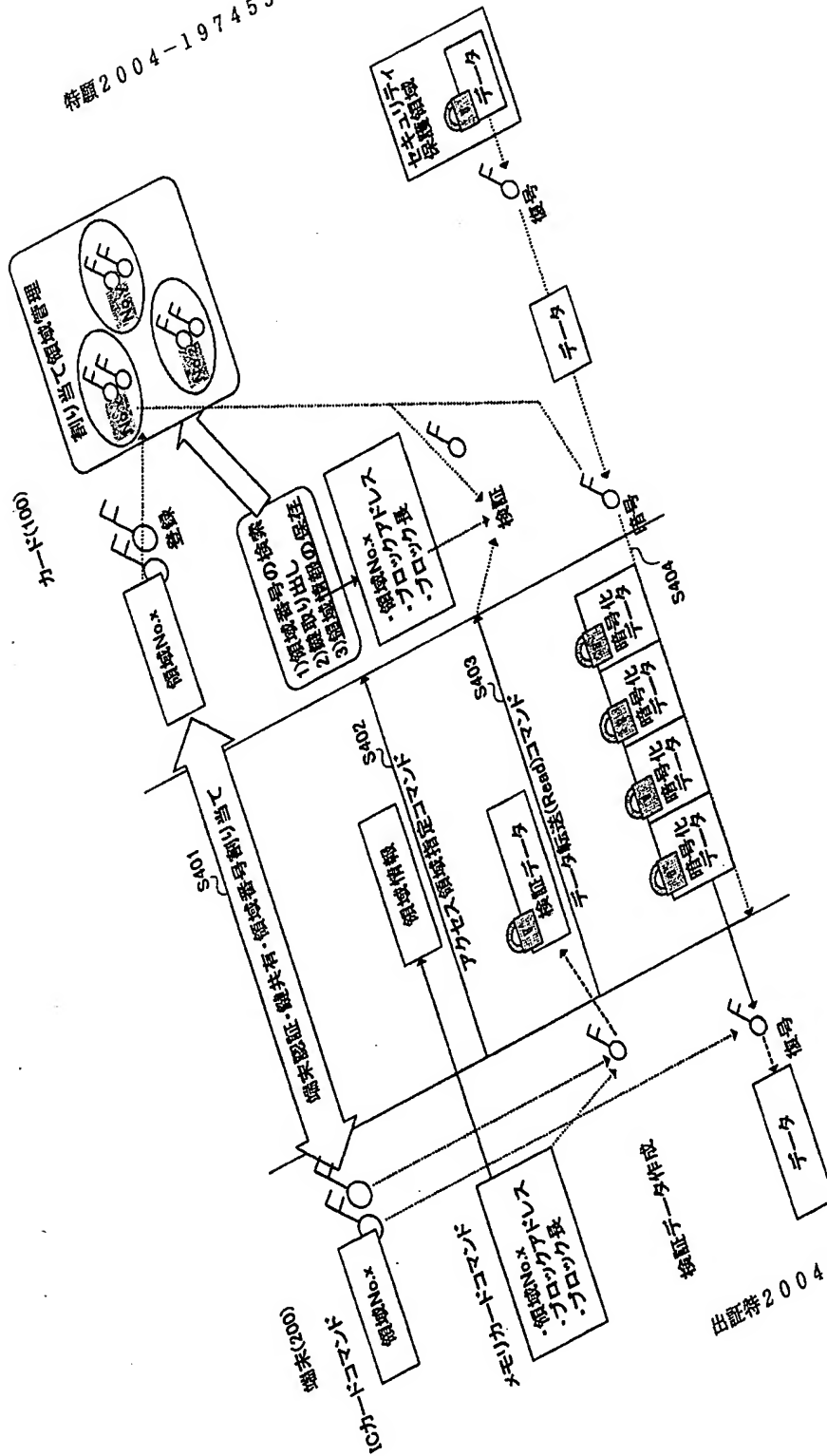
【図2】



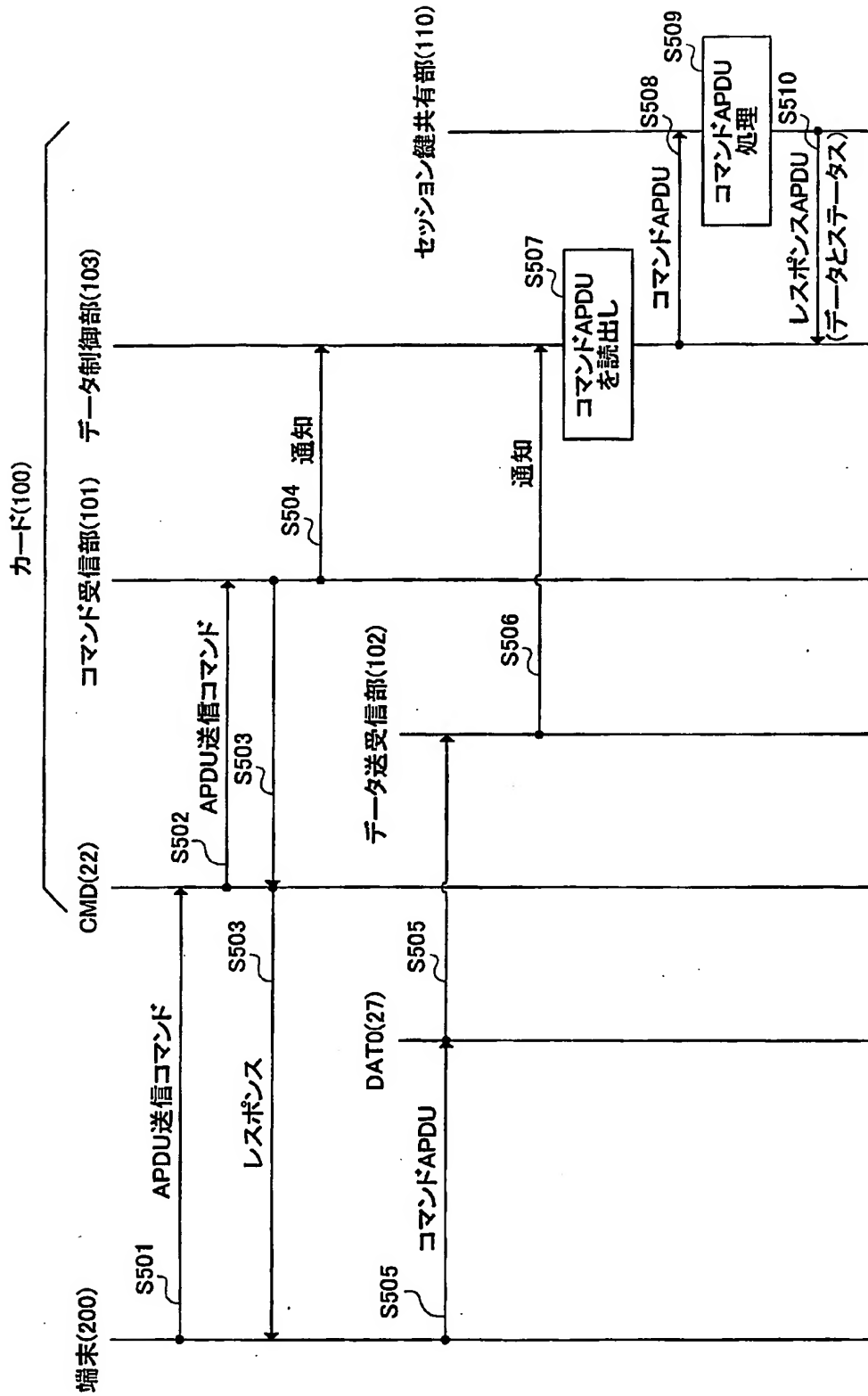
【図3】



【図4】

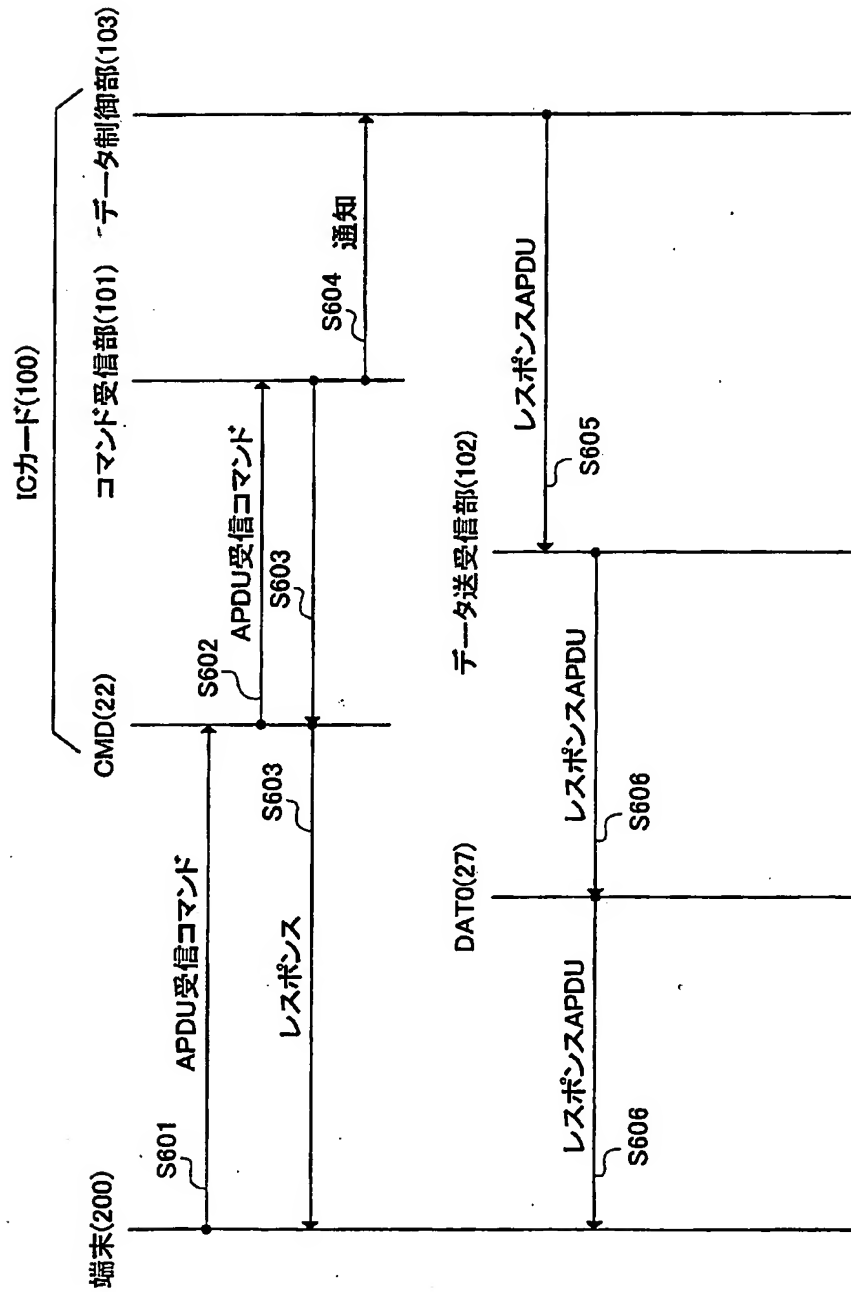


【図5】

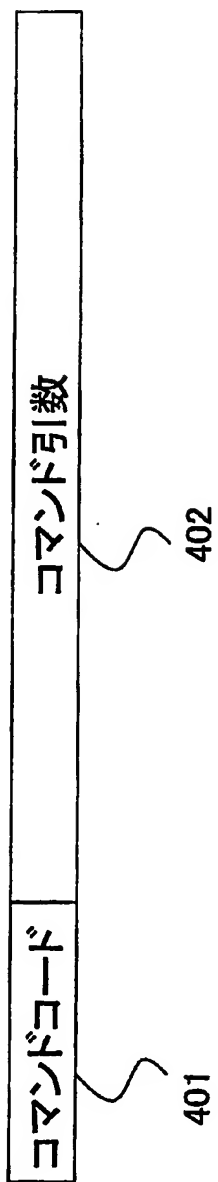




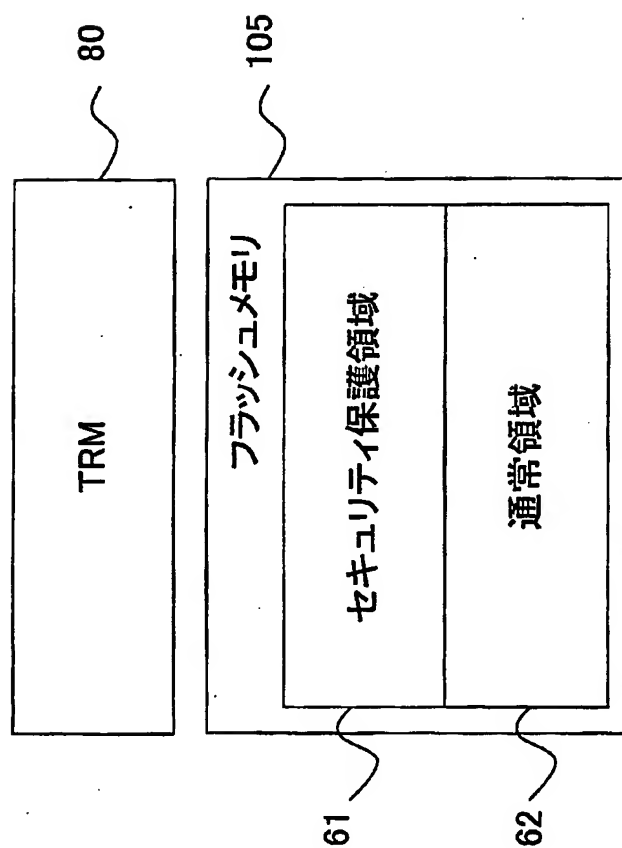
【図6】



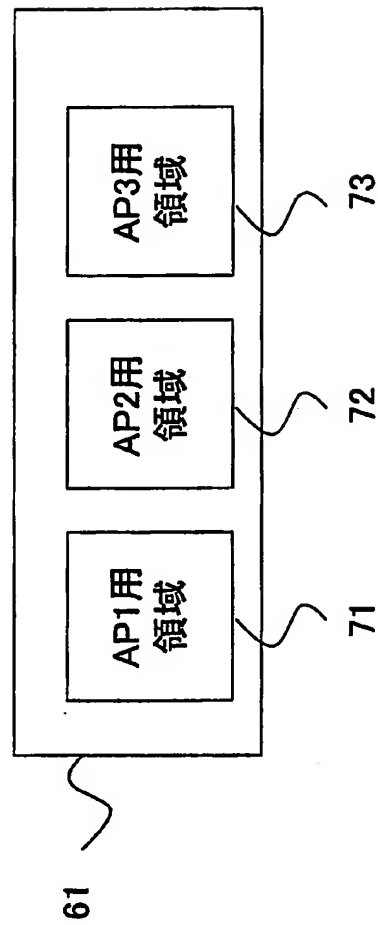
【図7】



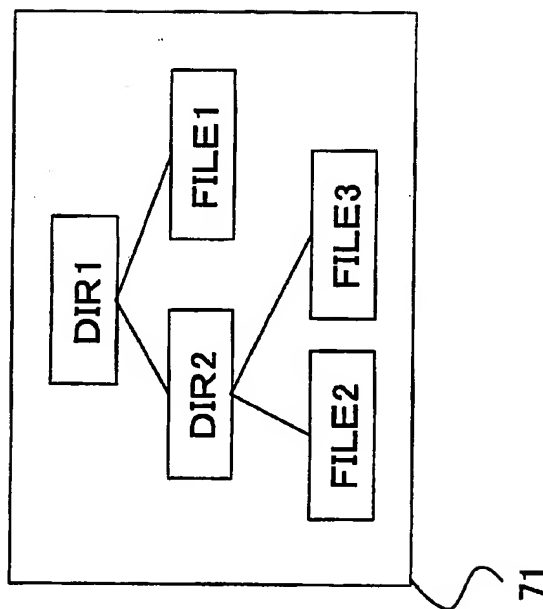
【図8】



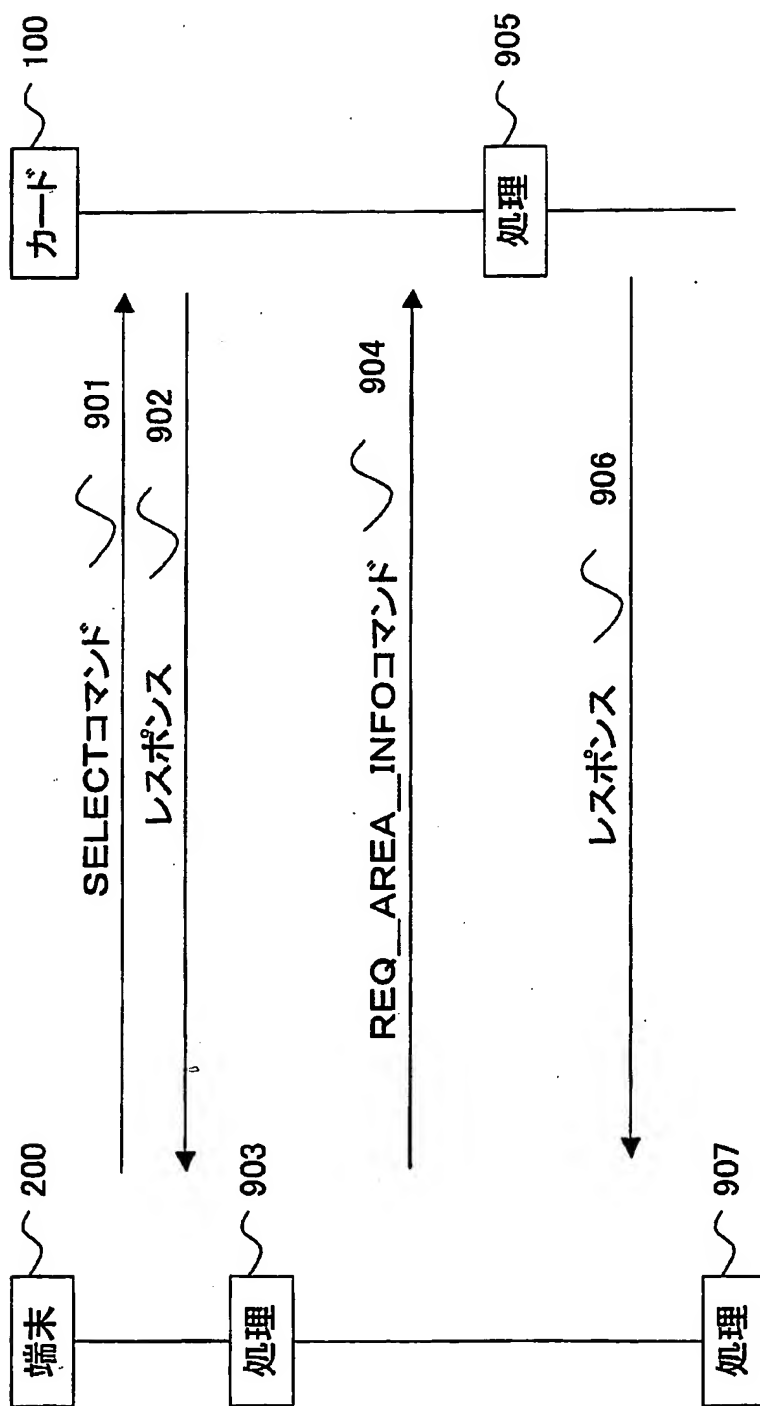
【図9】



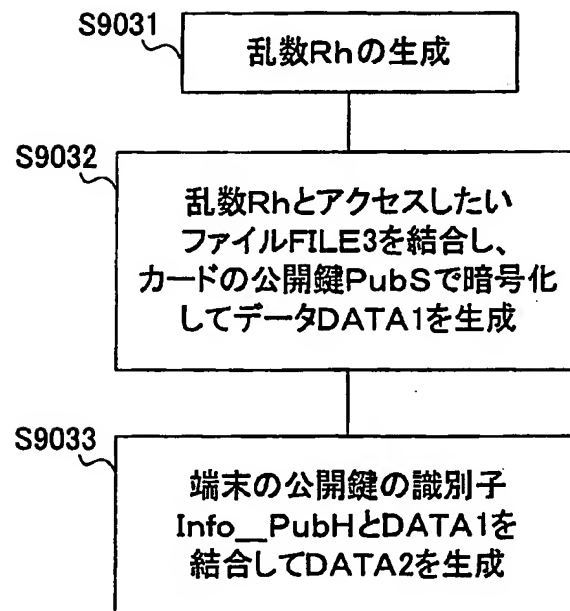
【図10】



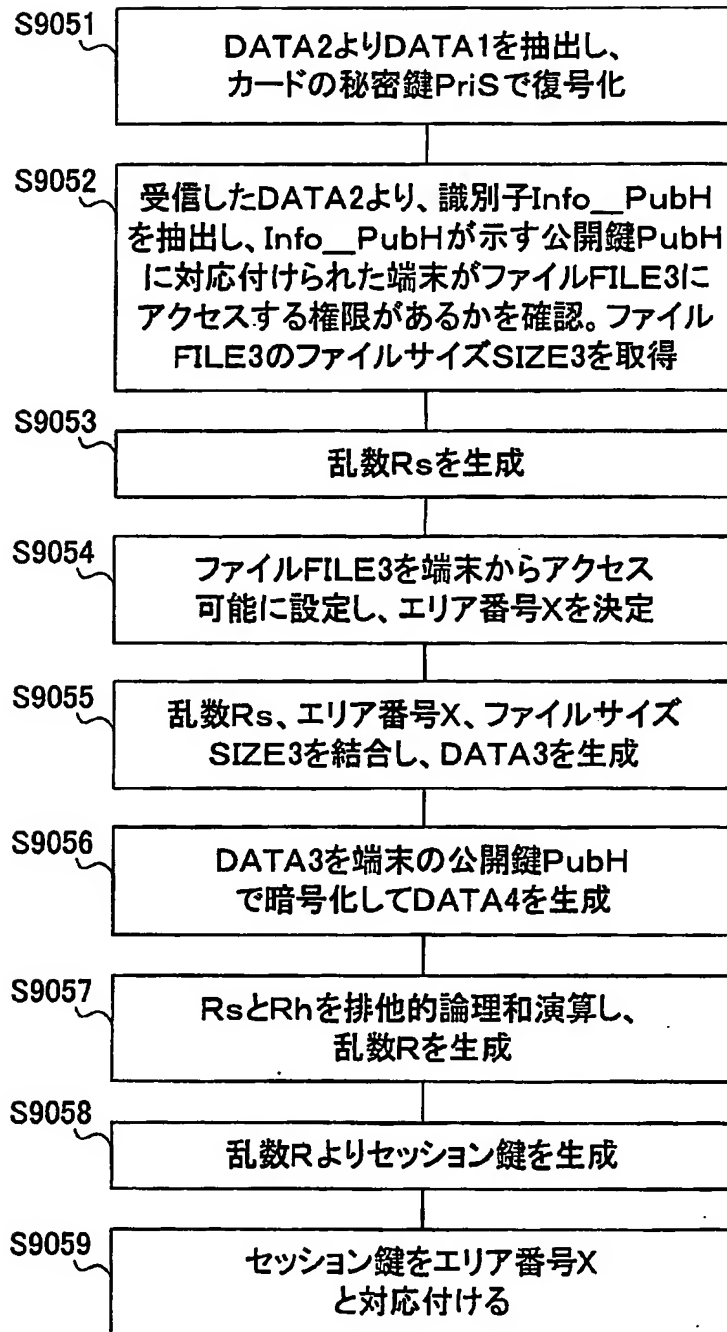
【図11】



【図12】

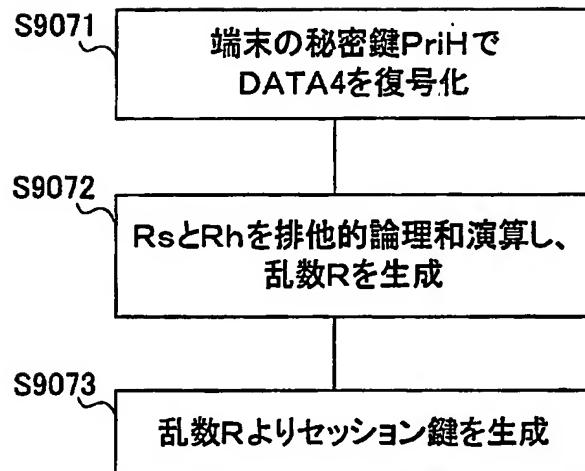


【図13】

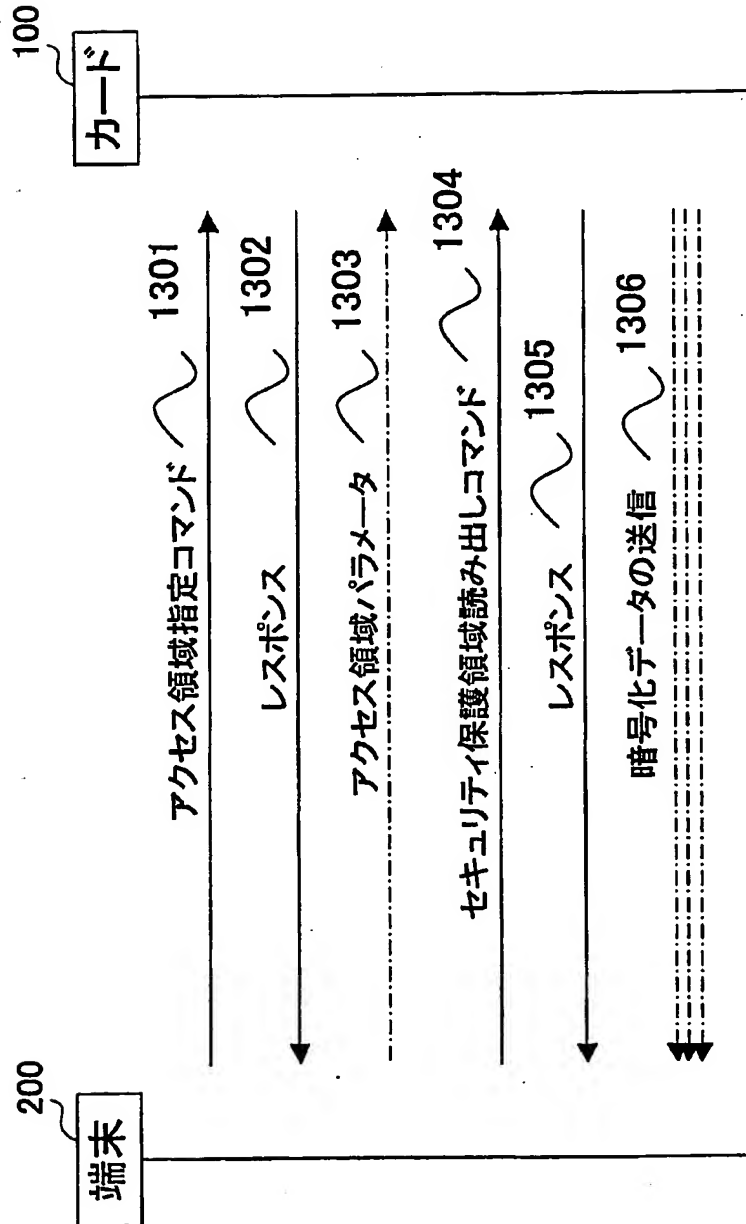




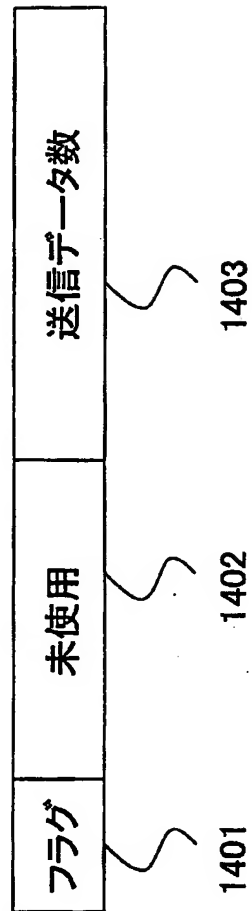
【図14】



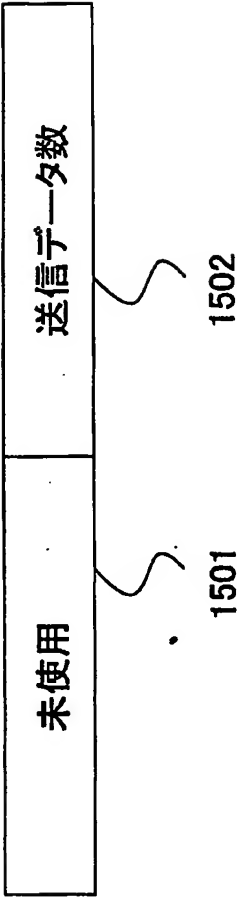
【図15】



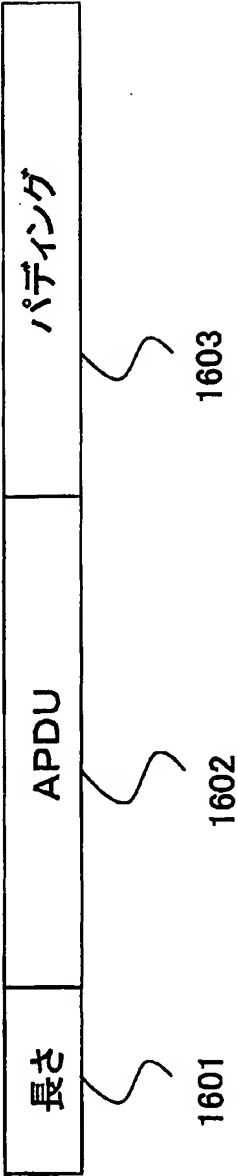
【図 16】



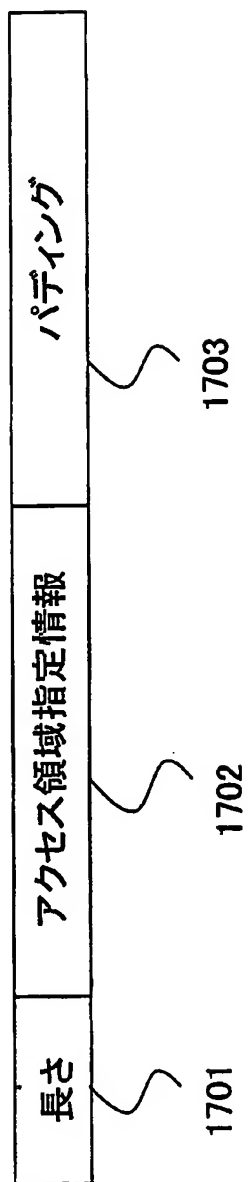
【図17】



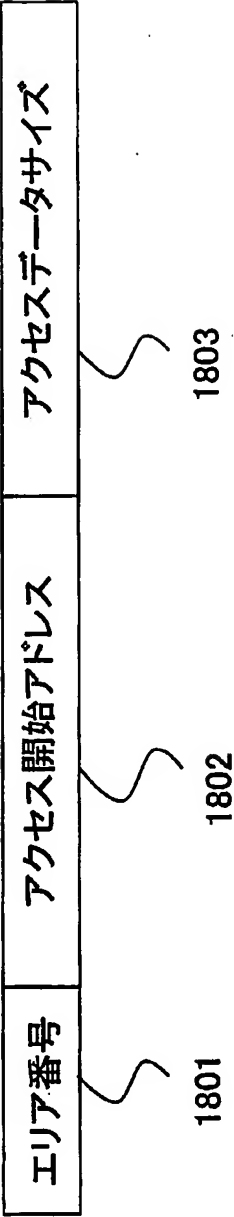
【図18】



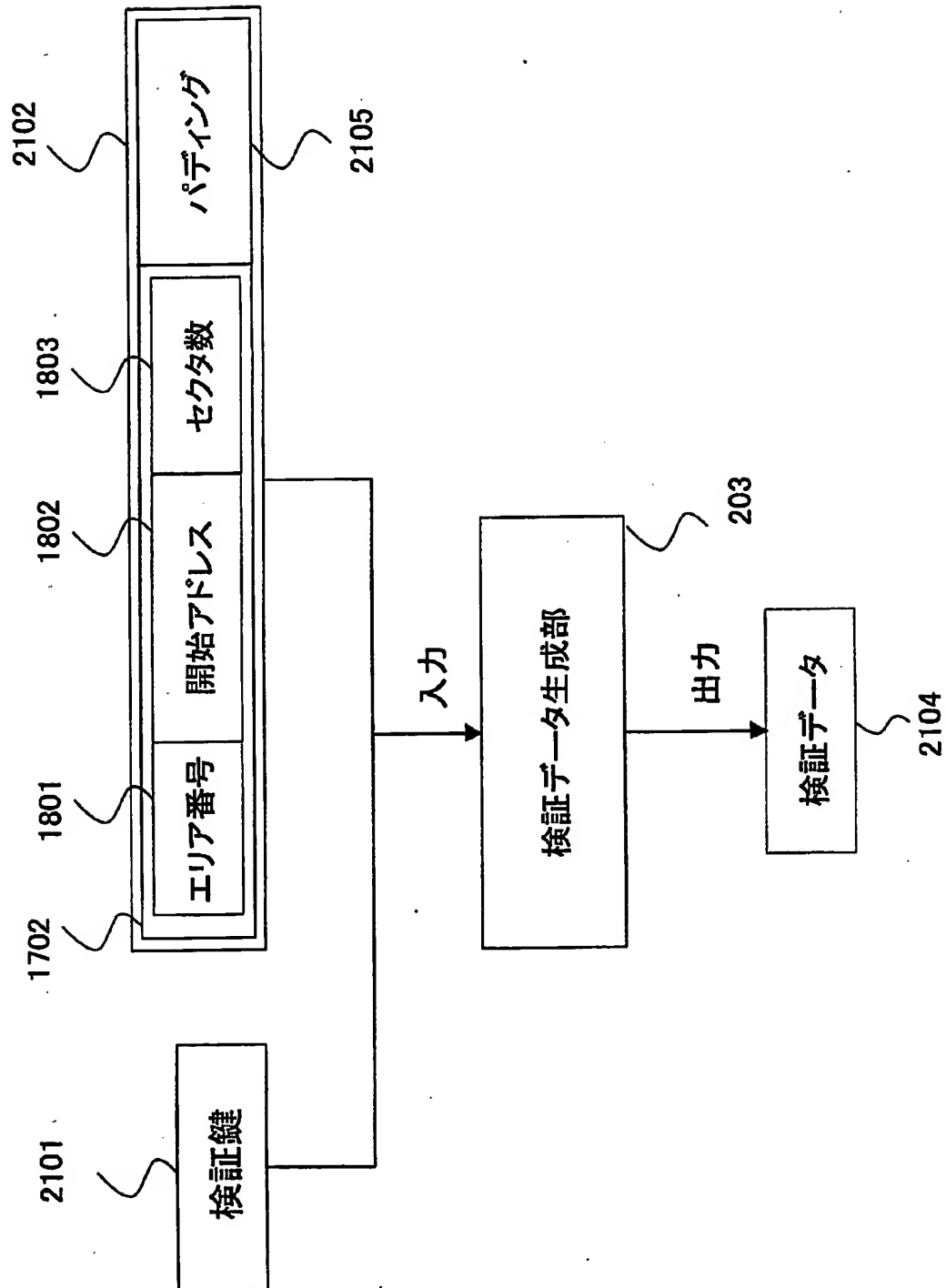
【図 19】



【図 20】

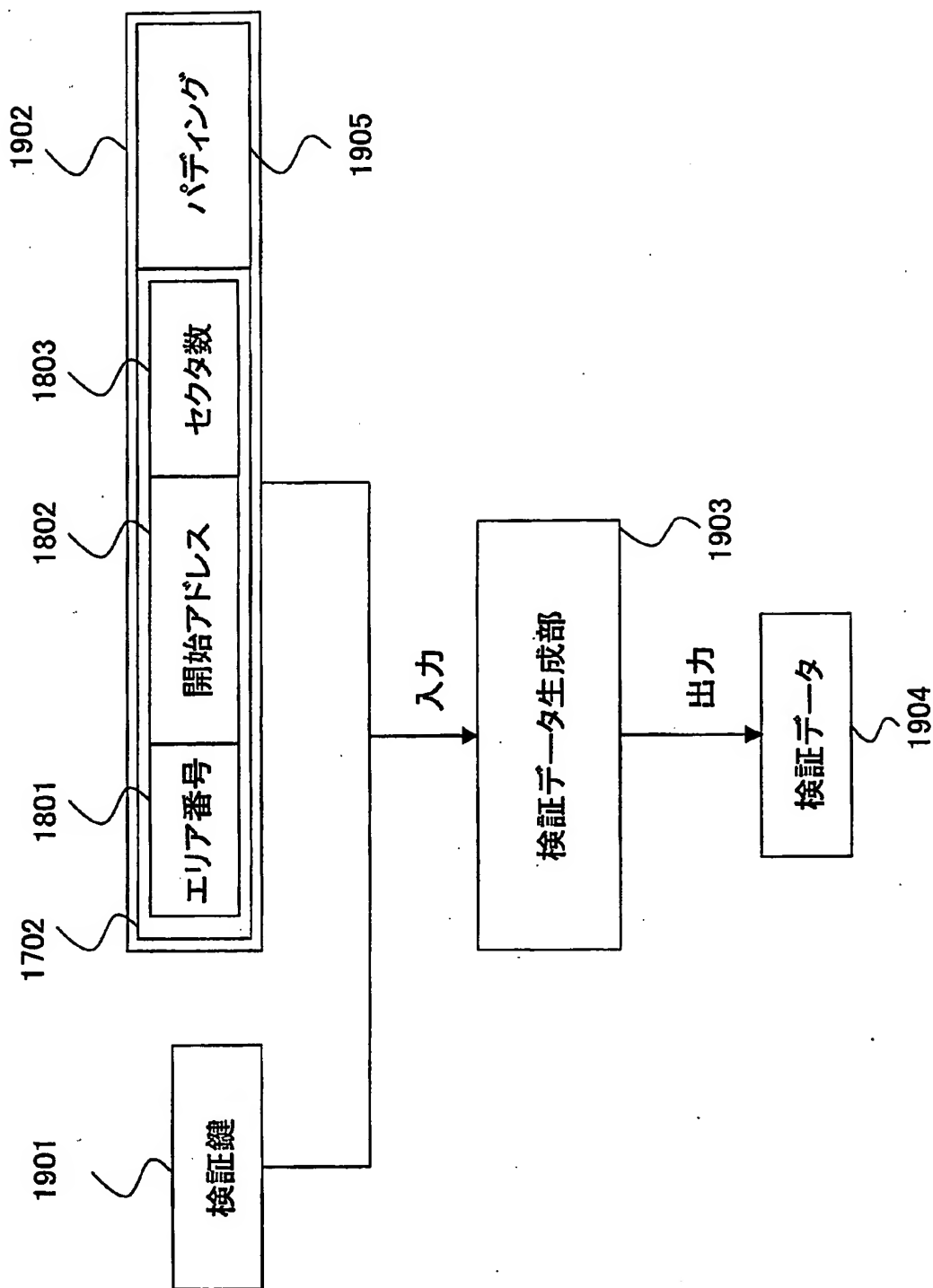


【図21】

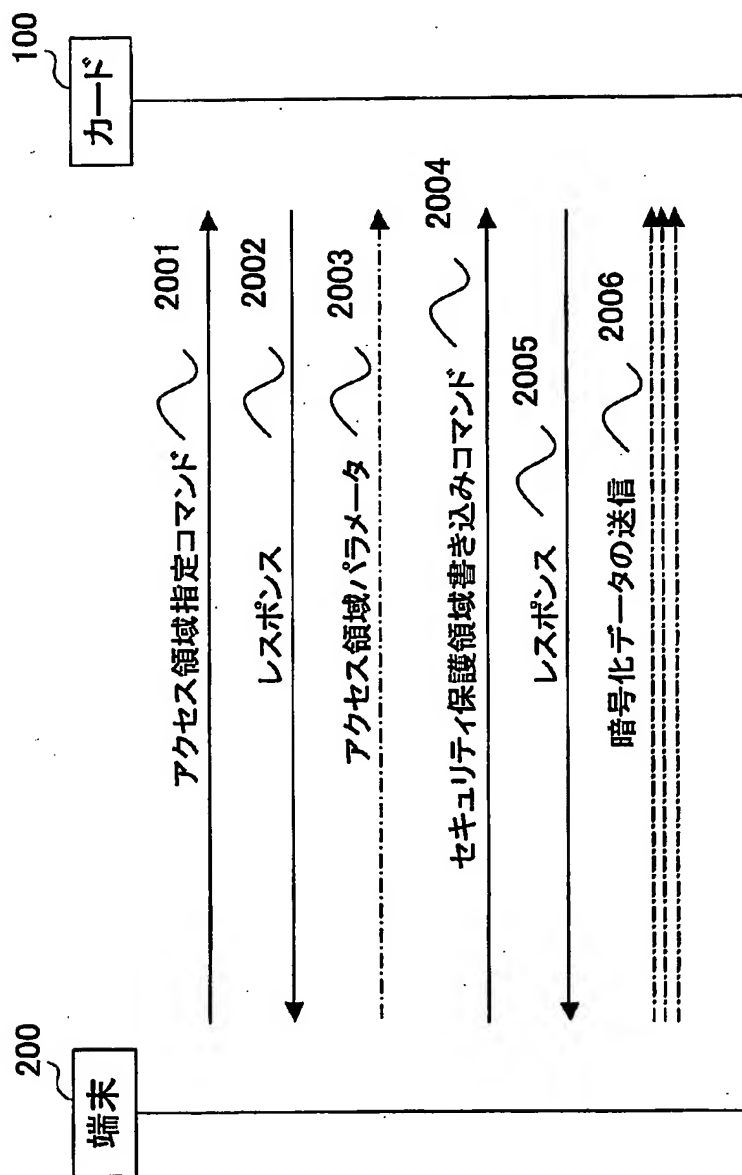




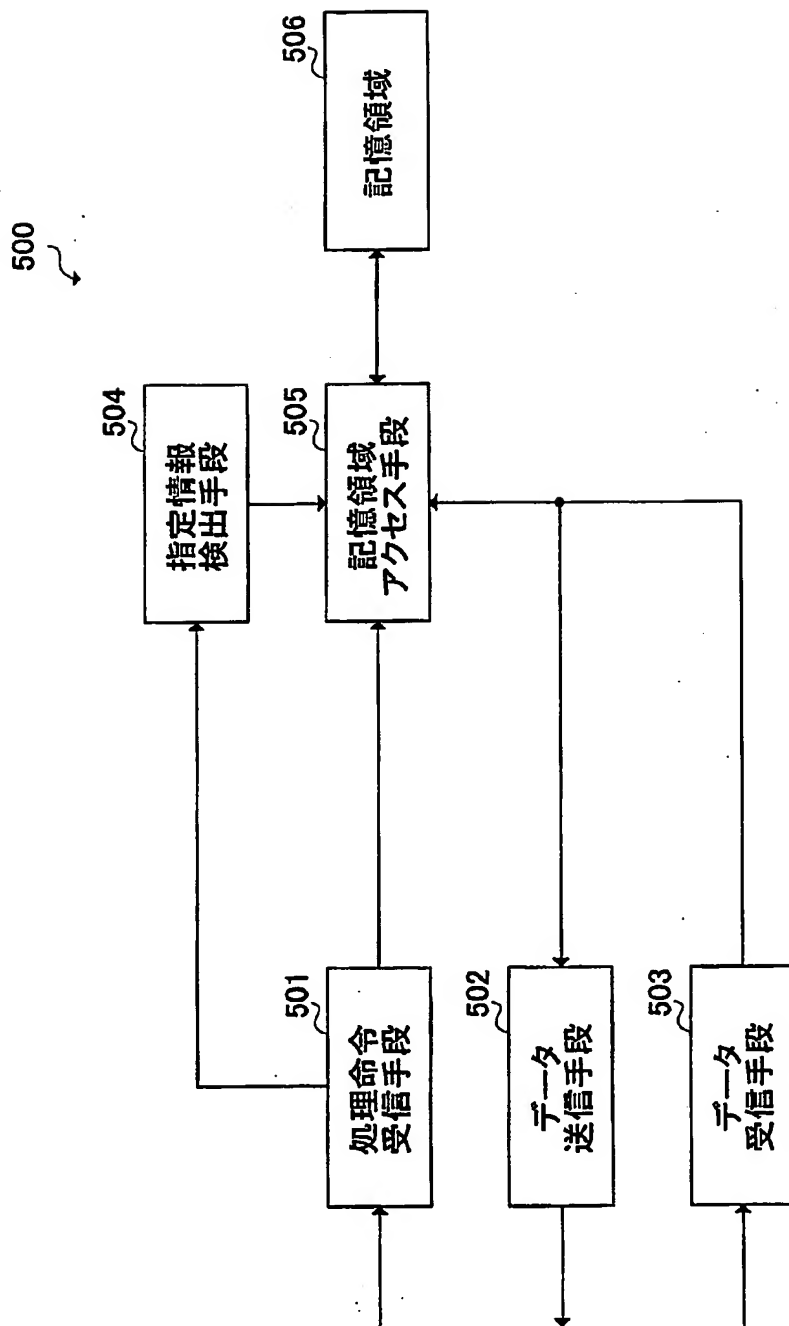
【図22】



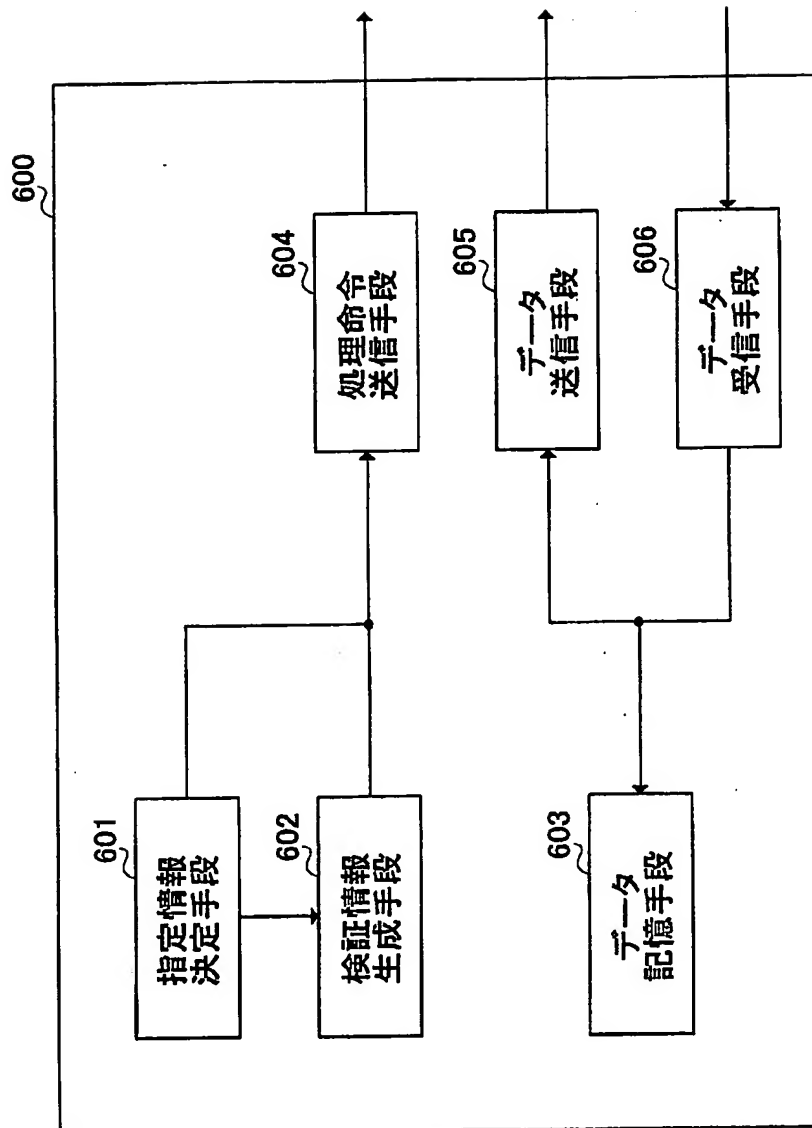
【図 23】



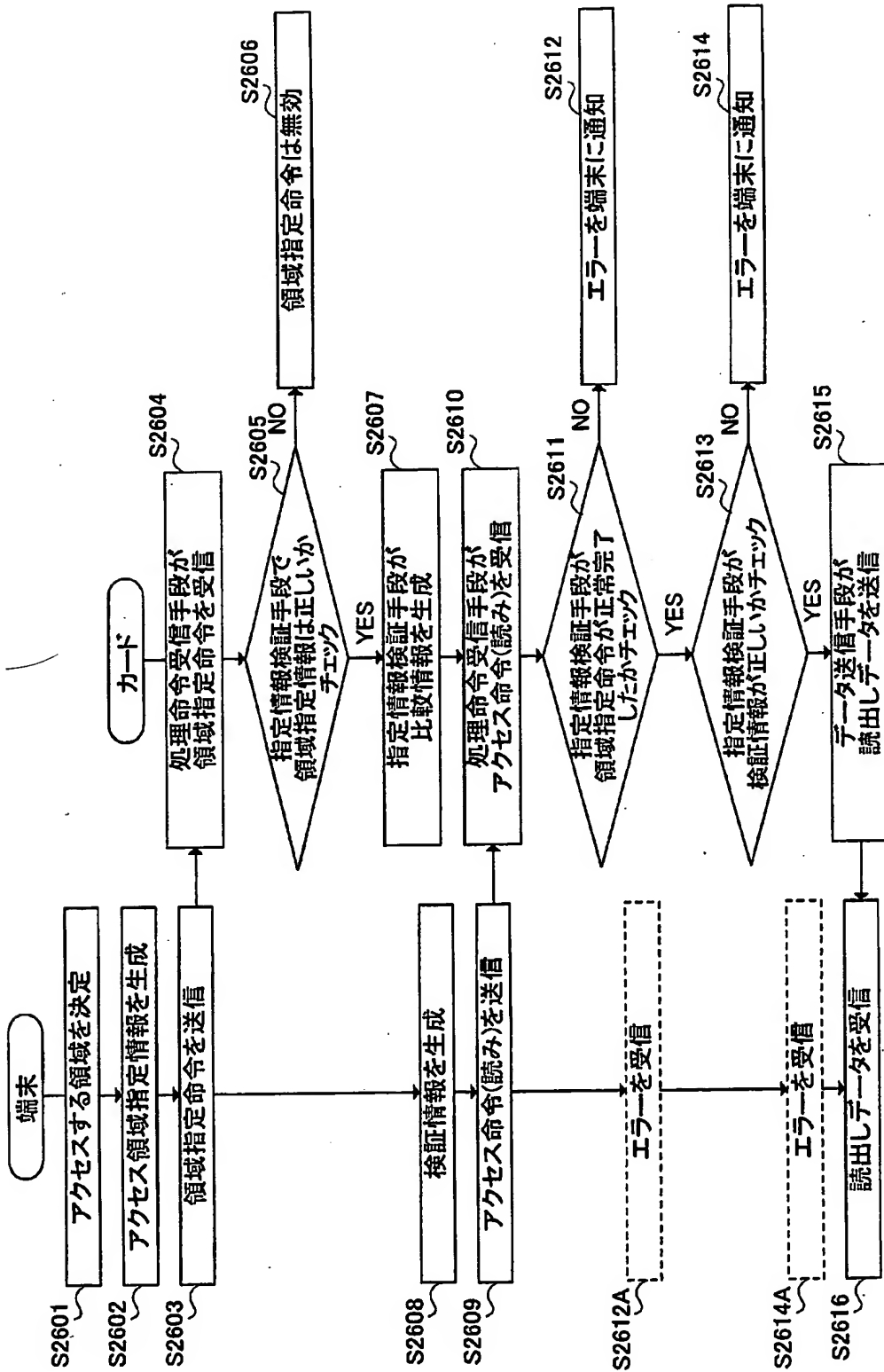
【図24】



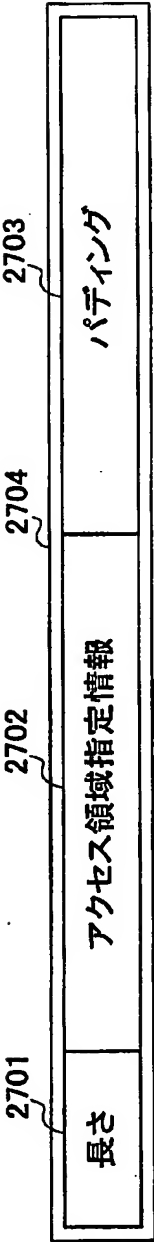
【図25】



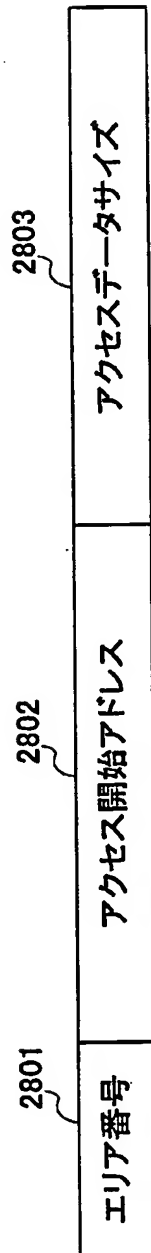
【図 26】



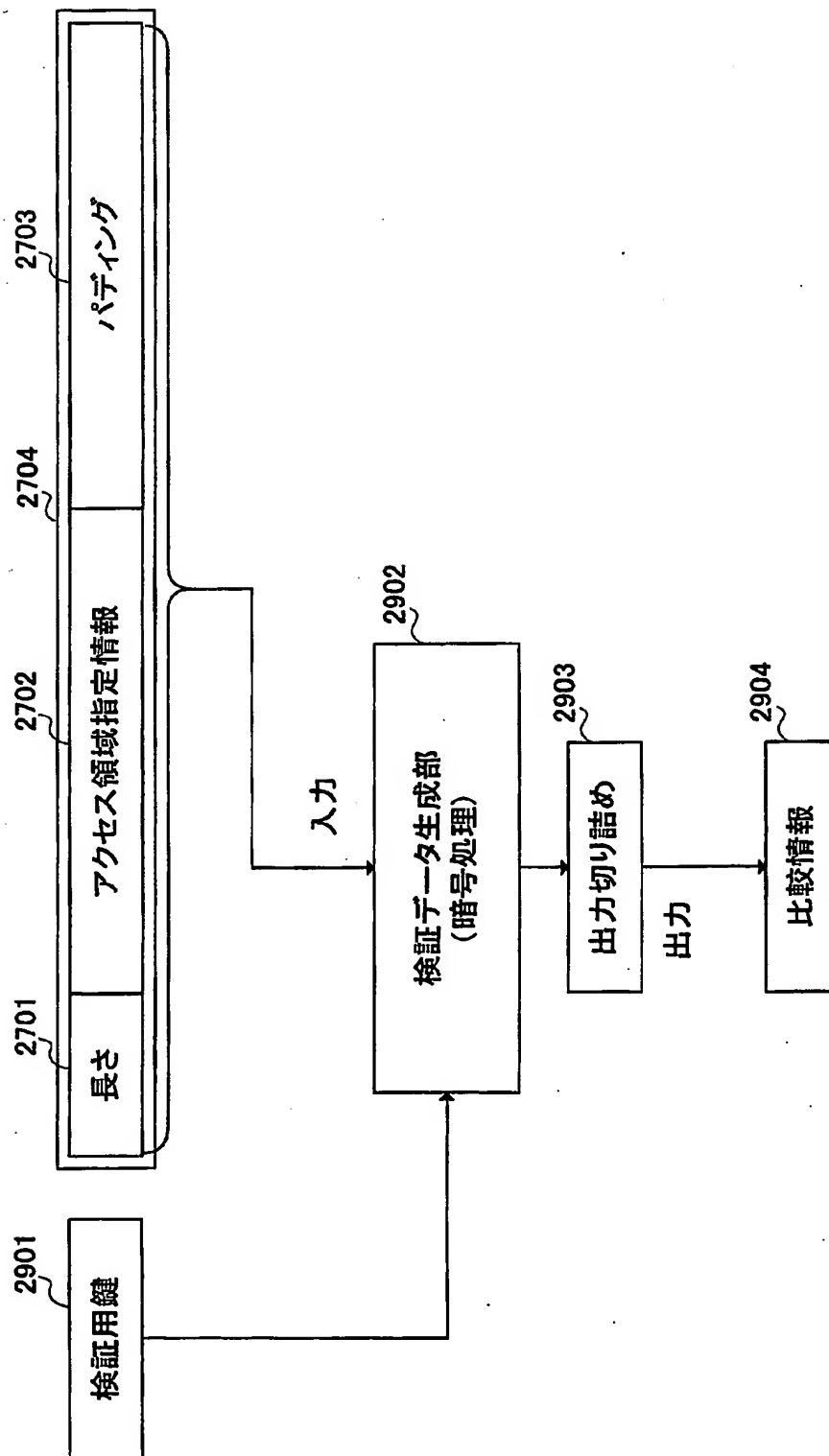
【図 2.7】



【図 28】

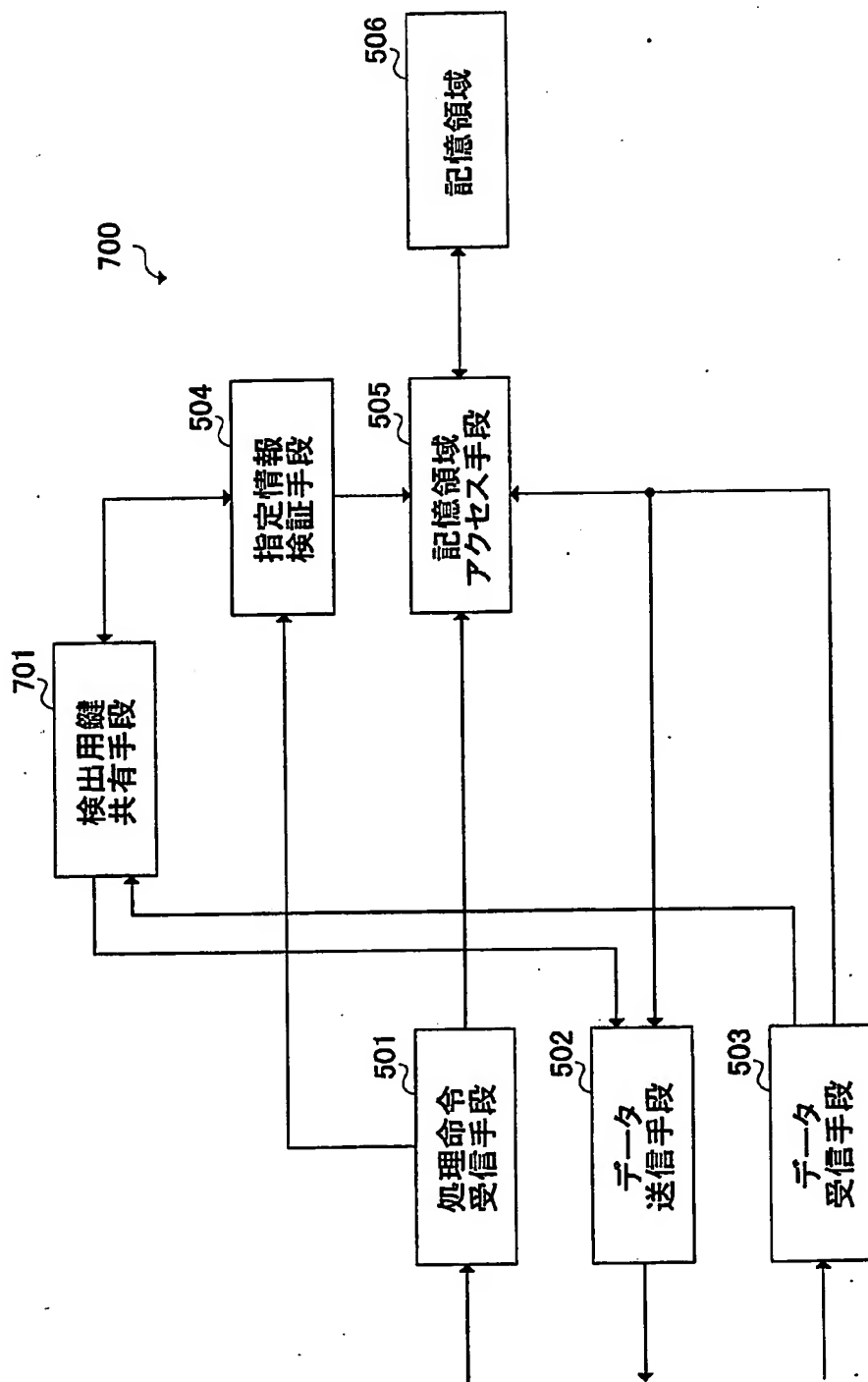


【図 29】

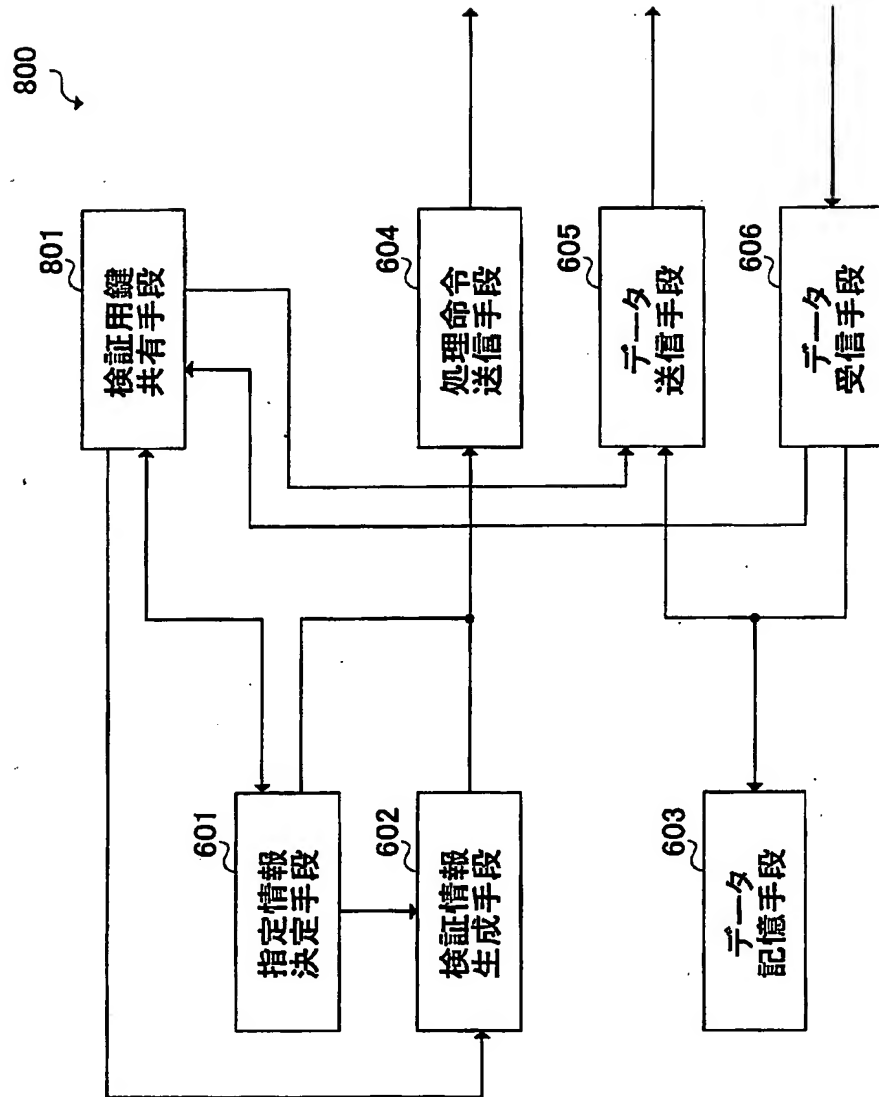




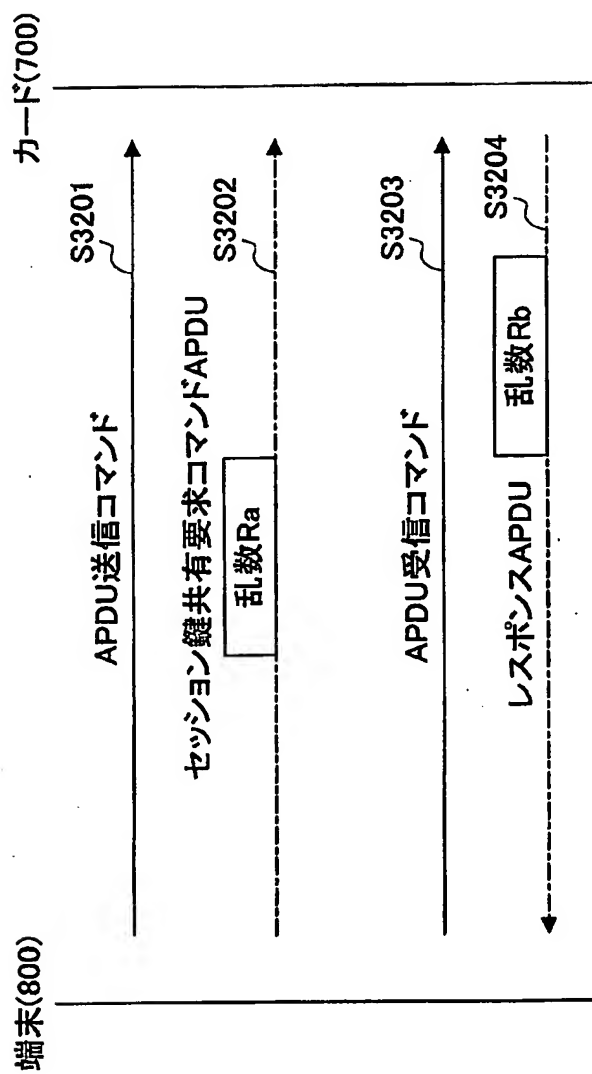
【図 30】



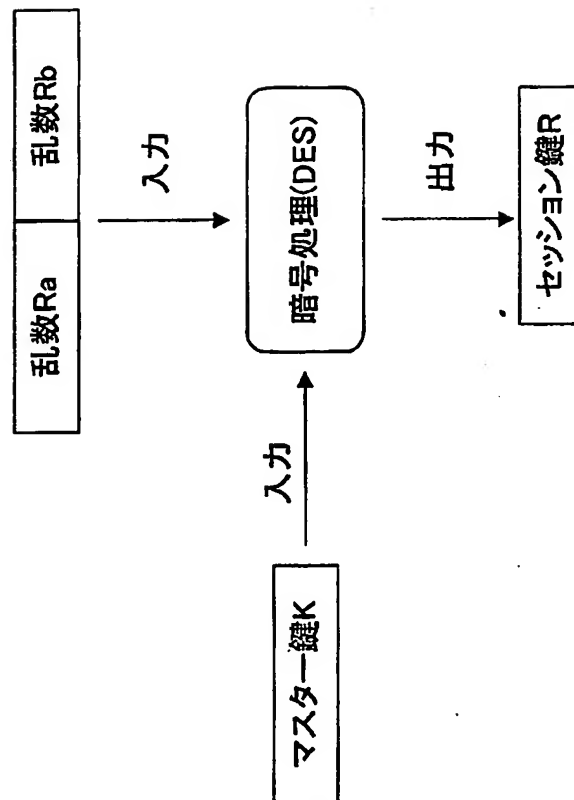
【図 31】



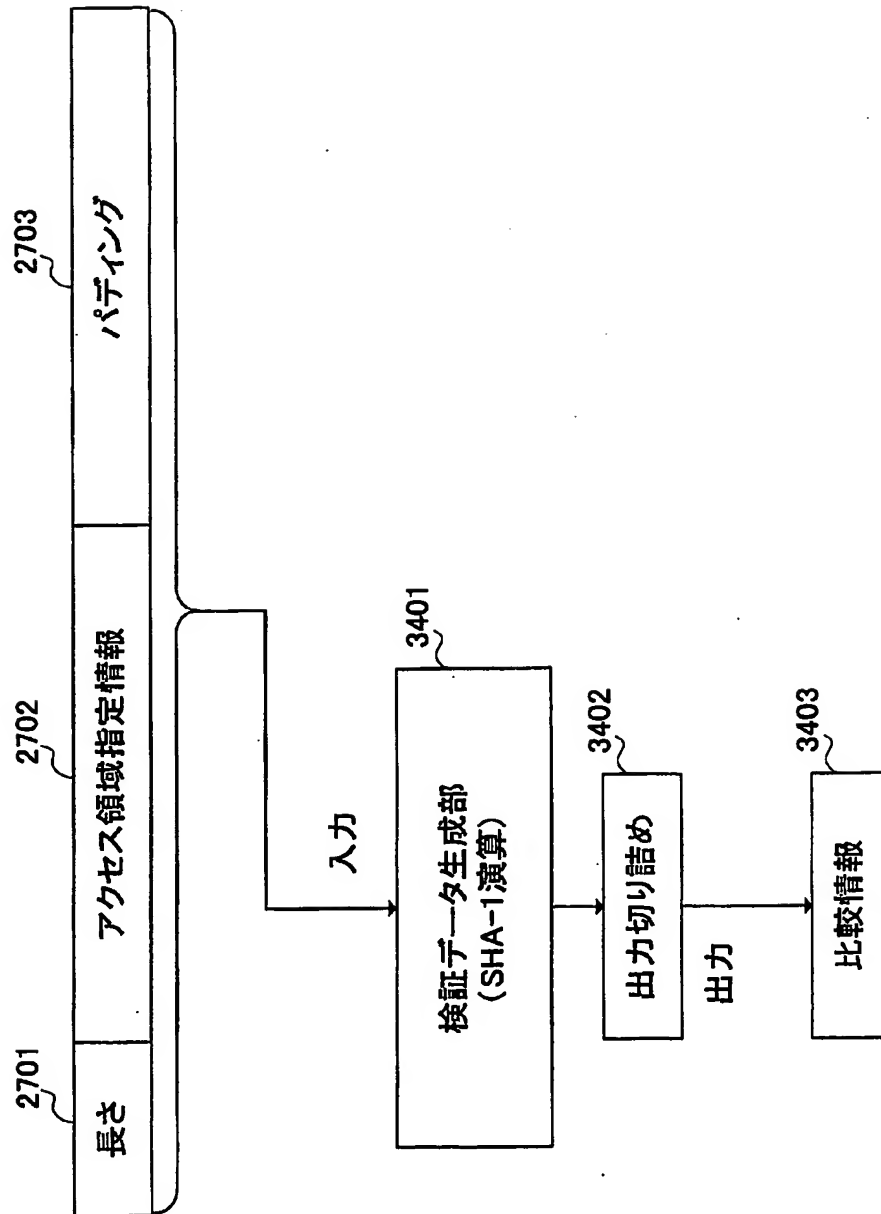
【図32】



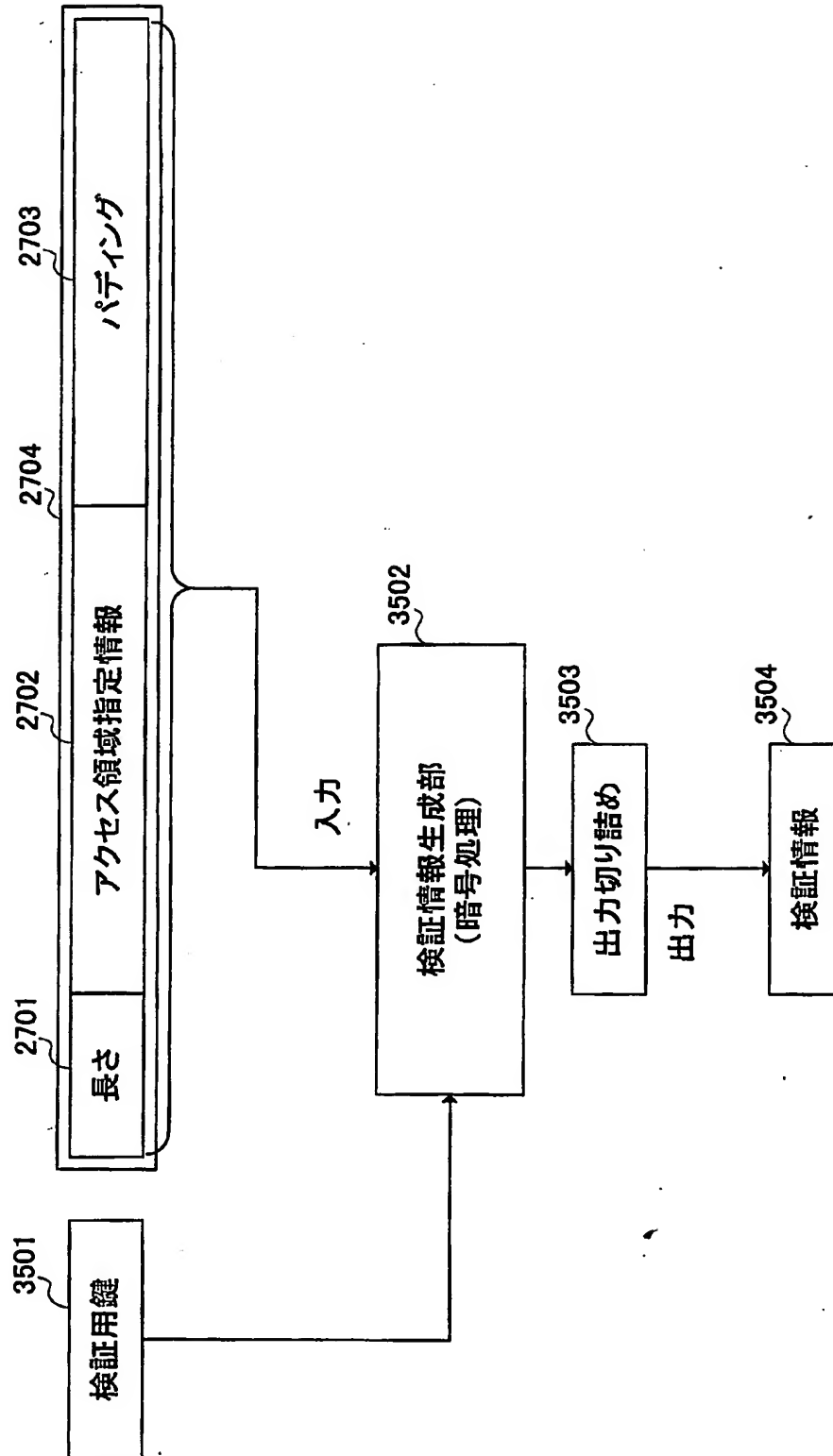
【図33】



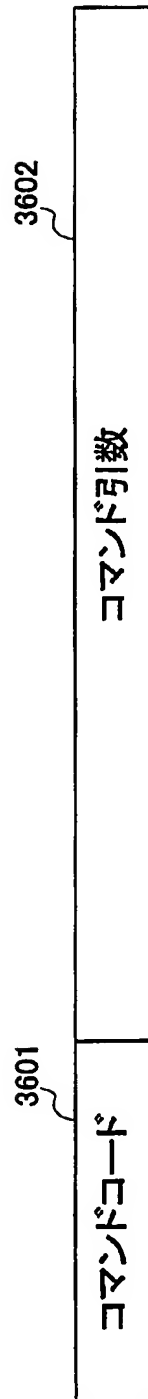
【図34】



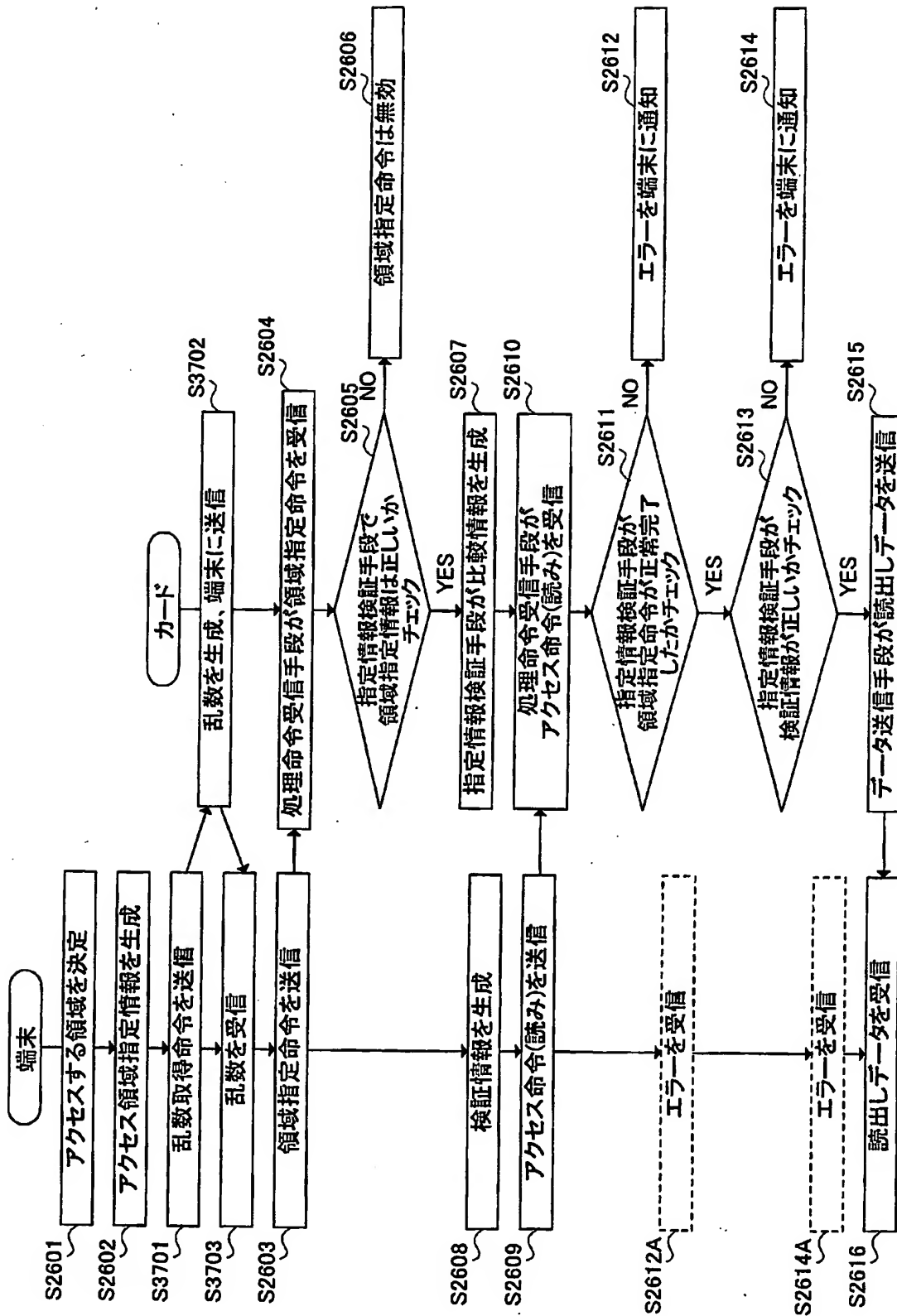
【図 35】



【図36】

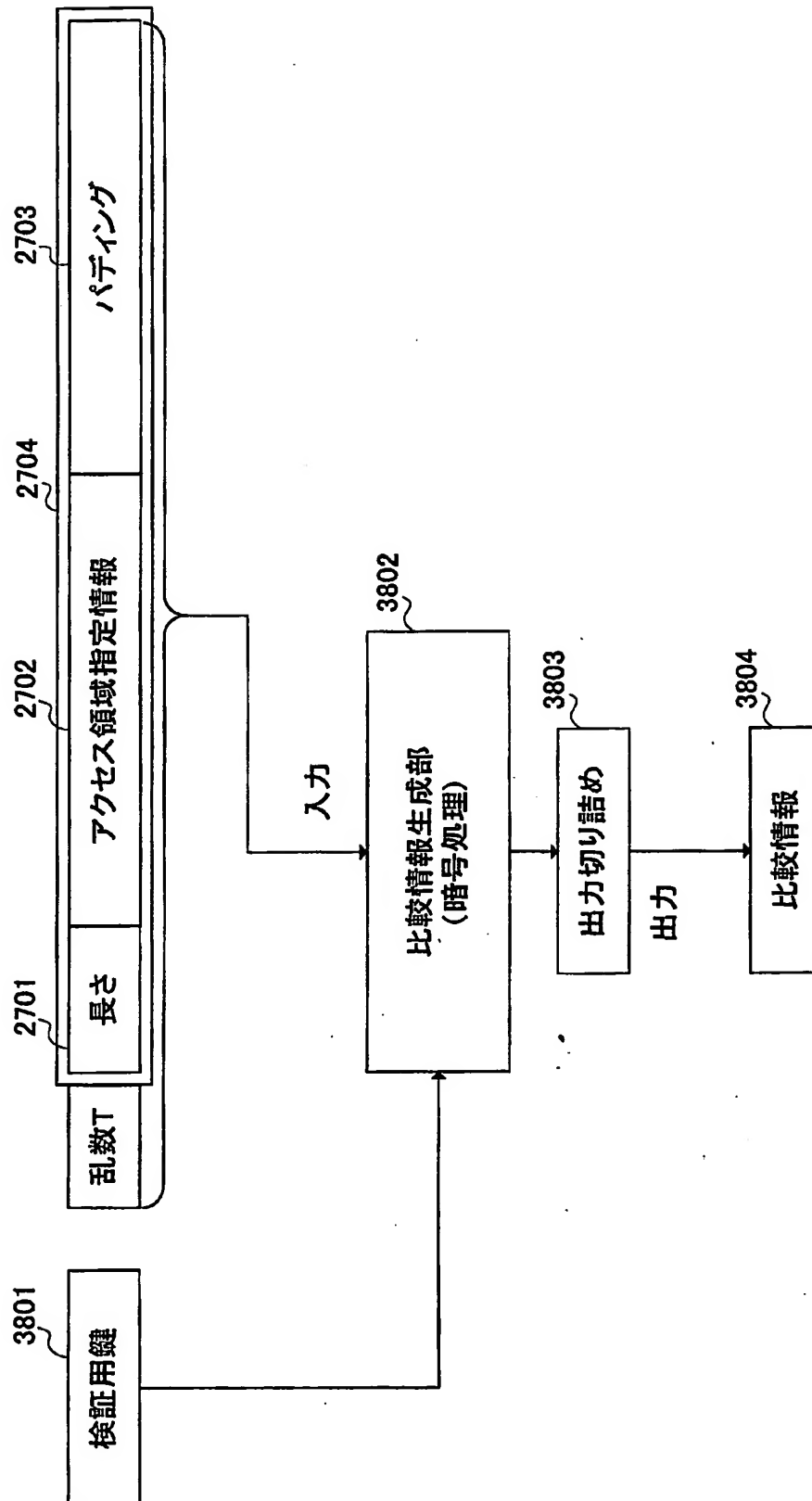


【図37】

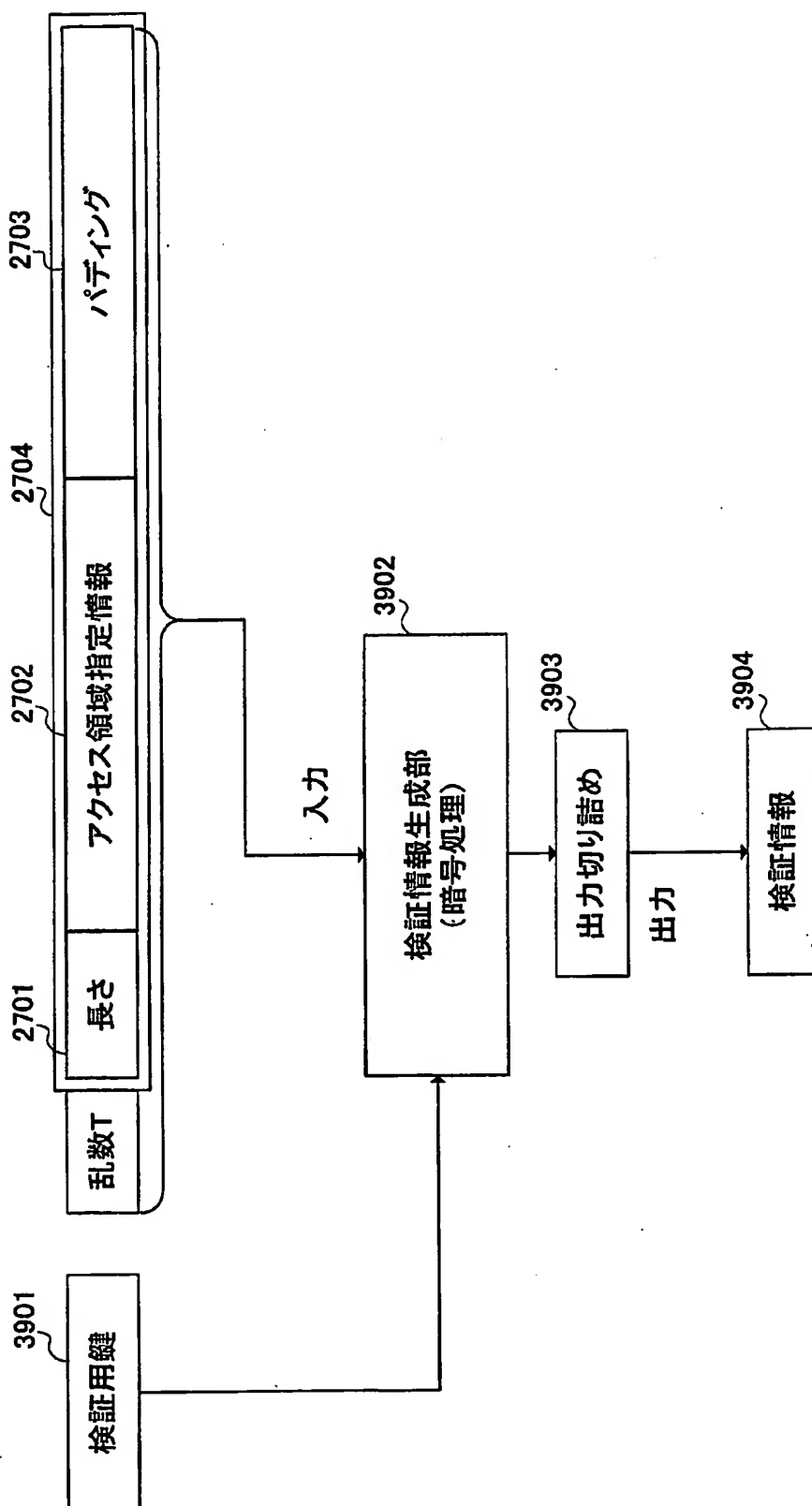




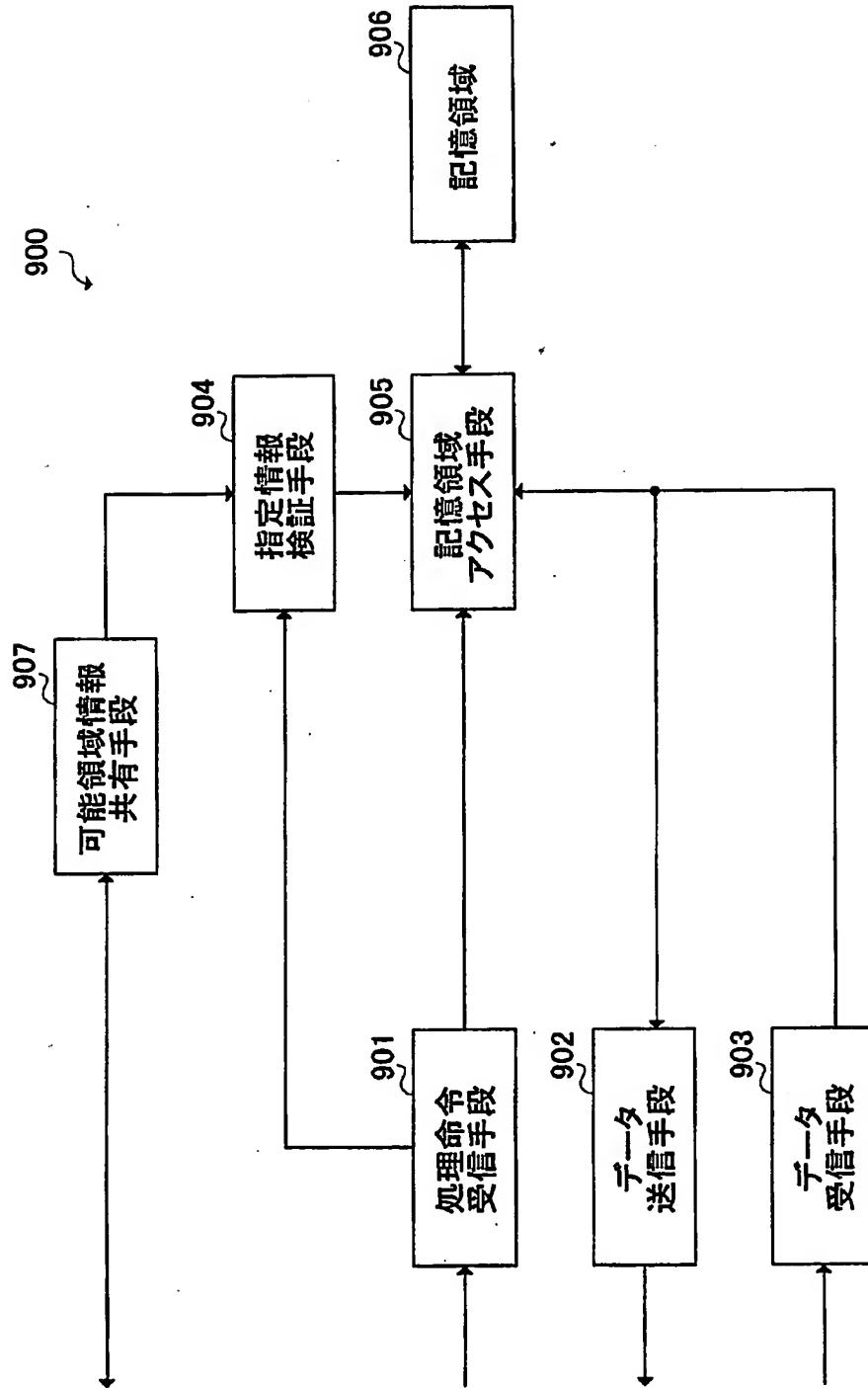
【図38】



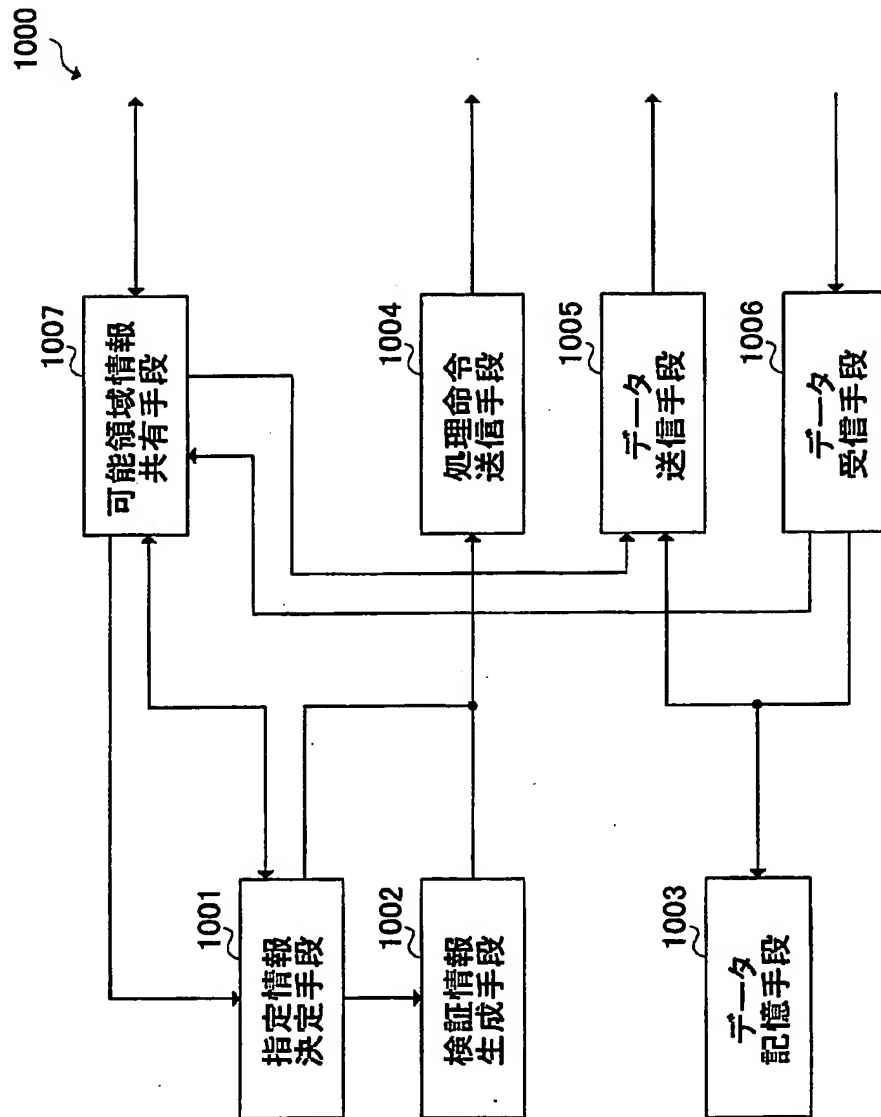
【図39】



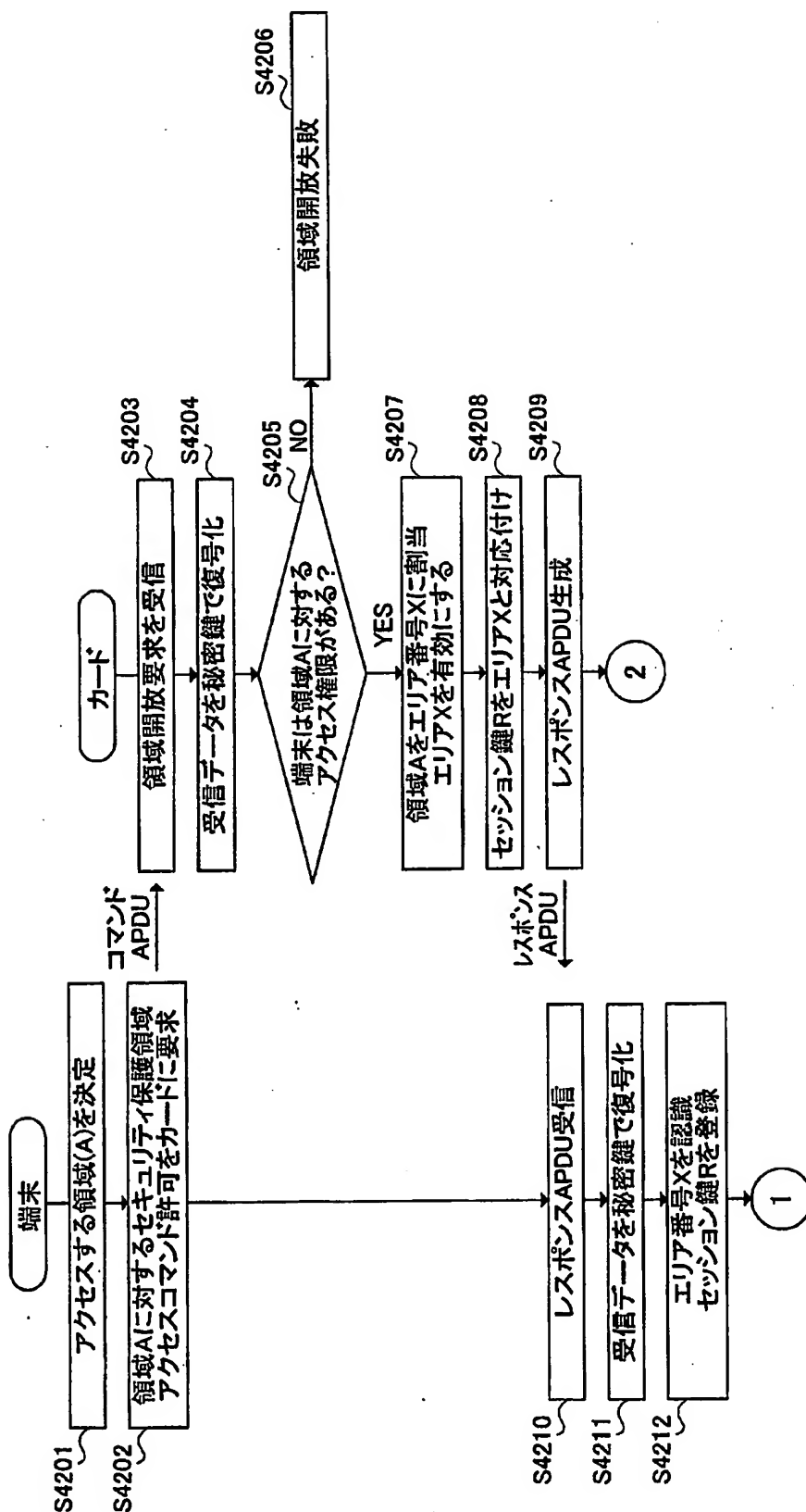
【図40】



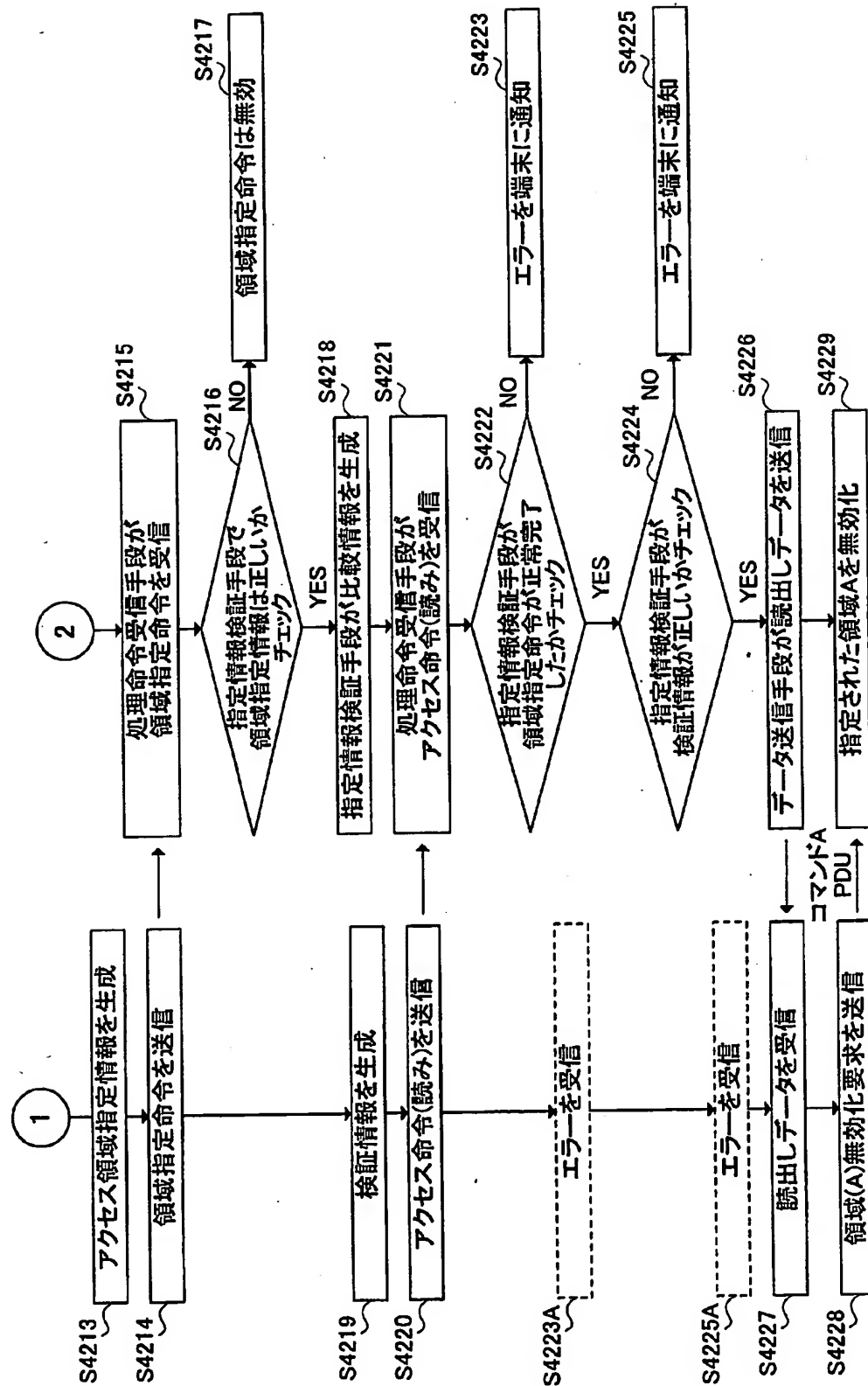
【図41】



【図 42】



【図43】



【図44】

4400  
↙

エリア番号X	領域識別子a	検証用鍵R
エリア番号2	領域識別子b	検証用鍵
エリア番号3	領域識別子c	検証用鍵
...	...	...

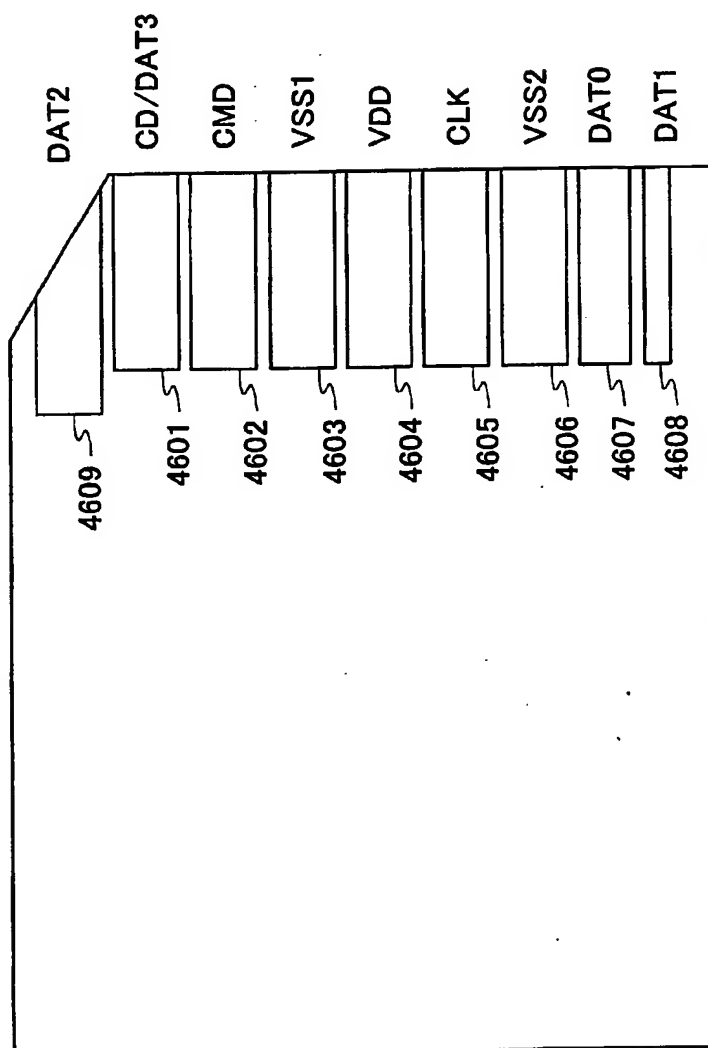
【図45】

4500  
↘

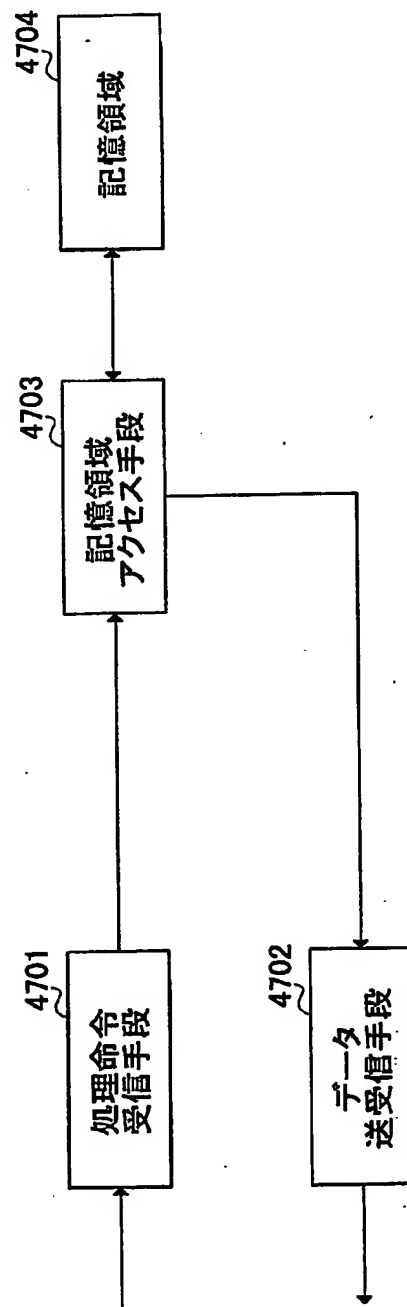
エリア番号X	FILE3	セッション鍵Km
エリア番号2	ファイル識別子2	セッション鍵
エリア番号3	ファイル識別子4	セッション鍵
...	...	...



【図 46】



【図 47】



【書類名】要約書

【要約】

【課題】 コマンド引数の小さいメモリカードコマンドにおいて、アクセス権限をもった端末を安全に認証可能とする。

【解決手段】 端末からアクセス領域を指定するコマンドと、アクセスを行うコマンドを分離し、アクセスを行うコマンドの引数に端末の検証データを含めて送信することで、アクセス領域を指定するコマンドを発行した端末アプリケーションとアクセスを行うコマンドを発行した端末アプリケーションと、検証用鍵を保有する端末アプリケーションが同一であることが検証可能となる。

【選択図】 図1

特願 2004-197453

出願人履歴情報

識別番号

[000005821]

1. 変更年月日

1990年 8月28日

[変更理由]

新規登録

住所

大阪府門真市大字門真1006番地

氏名

松下電器産業株式会社